QUI NIMIUS VOLLET
NIHIL CONSEQUITUR

ATLANTE DELL'AFFIDABILITÀ DIGITALE

OGNI NAZIONE

Rapporto annuale sul grado di sicurezza digitale, cooperazione tecnologica e condivisione dei dati

208 nazioni analizzate



FONDAZIONE OLIVETTI TECNOLOGIA E RICERCA

Capo progetto: Nicolini Massimiliano

Destinatari: Istituzioni italiane

ATLANTE DELL'AFFIDABILITA DIGITALE

OGNI NAZIONE

Rapporto annuale sul grado di sicurezza digitale, cooperazione tecnologica e condivisione dei dati

Edizione Celeborn Intelligence estesa 2026 - revisione AI Act, legge 132/2025 e cybercrime

Autore istituzionale	Fondazione Olivetti Tecnologia e Ricerca
Capo progetto	Nicolini Massimiliano
Destinatari	Istituzioni italiane
Edizione	2026
Chiusura editoriale	5 agosto 2026

Natura del documento

Valutazione comparativa basata su informazioni pubblicamente accessibili. Il volume non contiene informazioni classificate e non sostituisce pareri legali, determinazioni di sicurezza nazionale, controlli sanzionatori, golden power, autorizzazioni all'esportazione o verifiche tecniche sul singolo fornitore.

QUI NIMIUS VOLLET NIHIL CONSEQUITUR

Nota editoriale

L'Atlante dell'affidabilità digitale nasce come periodico annuale di orientamento strategico destinato alle istituzioni italiane, agli enti pubblici, alle imprese che operano con infrastrutture o dati sensibili e ai soggetti impegnati in cooperazione tecnologica internazionale. La domanda centrale non è quale Paese disponga delle tecnologie più avanzate in assoluto, ma in quale misura un operatore italiano possa utilizzare, acquistare, integrare o condividere dati con quell'ecosistema mantenendo controllo giuridico, sicurezza, continuità e libertà di uscita.

L'edizione 2026 include 208 Stati, territori ed entità a riconoscimento pieno, parziale o de facto. L'inclusione non costituisce riconoscimento diplomatico e serve esclusivamente a evitare zone cieche operative. Ogni capitolo combina una premessa geopolitica collegata alla tecnologia, dati comparabili, analisi delle infrastrutture e dell'intelligenza artificiale, capitale umano, supply chain, postura cyber, libertà digitale, norme, tecnologie civili, governative e militari, trasferimenti dall'Italia, scorecard e matrice di rischio.

Il risultato è una guida di valutazione preliminare. Un punteggio elevato non elimina la verifica preventiva sul fornitore; un punteggio basso non attribuisce condotte illecite a un Paese o a un'azienda, ma segnala che l'onere di prova, le garanzie e le autorizzazioni devono essere più forti. Le valutazioni sono rivedibili in presenza di nuove leggi, conflitti, sanzioni, accordi tecnologici, incidenti, cambi di governo o mutamenti nelle catene di fornitura.

Premessa del capo progetto

Perché misurare la fiducia digitale tra le nazioni

La sicurezza digitale non è più una funzione tecnica confinata ai sistemi informativi. È diventata una componente della sovranità, della continuità dello Stato, della tutela dei cittadini e della capacità economica di scegliere con chi condividere dati, conoscenza, infrastrutture e processi decisionali. Ogni collaborazione tecnologica internazionale apre opportunità, ma introduce anche dipendenze giuridiche, industriali e geopolitiche che devono essere rese visibili prima che diventino irreversibili.

L'Atlante dell'affidabilità digitale nasce per offrire alle istituzioni italiane un linguaggio comune. Non pretende di sostituire l'intelligence, la valutazione legale, l'audit tecnico o il controllo politico; li prepara. Trasforma una massa dispersa di informazioni aperte in un quadro leggibile, comparabile e aggiornabile, capace di indicare dove la cooperazione può procedere con strumenti ordinari e dove, invece, occorrono segregazione, autorizzazioni, garanzie rafforzate o rinuncia all'operazione.

Il punto di osservazione è deliberatamente italiano. Un Paese può essere tecnologicamente avanzato e, nello stesso tempo, risultare difficile da integrare con le regole, le responsabilità e gli interessi strategici dell'Italia. Per questo il volume distingue la maturità tecnica dalla fiducia operativa: considera infrastrutture, intelligenza artificiale, capitale umano, supply chain e cybersecurity, ma anche trasferibilità dei dati, trasparenza, cooperazione probatoria, indipendenza delle autorità e possibilità concreta di applicare rimedi.

La nuova componente dedicata all'AI Act e alla legge 23 settembre 2025, n. 132 rende immediata una domanda che ogni amministrazione e impresa dovrebbe porsi prima di acquistare, sviluppare o integrare un sistema di intelligenza artificiale: quanto è distante l'ecosistema del Paese controparte dagli obblighi e dai principi ai quali noi dobbiamo rispondere? L'indicatore grafico non concede certificazioni preventive; segnala il livello di attrito normativo e organizzativo che dovrà essere colmato nel contratto, nell'architettura e nella governance.

Analoga importanza assume il cybercrime. Ransomware, frodi finanziarie, furto di credenziali, estorsione mediante sottrazione o cifratura dei dati, compromissione della supply chain e riciclaggio digitale non sono eventi separati dalla geopolitica tecnologica. Essi sfruttano infrastrutture, fornitori, giurisdizioni, asimmetrie investigative e opacità societarie. Conoscere la pressione criminale, gli attori prevalenti e la capacità di risposta del Paese è essenziale per stabilire dove conservare i log, chi possiede le chiavi, come notificare un incidente e quale cooperazione probatoria sia realisticamente ottenibile.

Questo Atlante deve quindi essere usato come strumento di prevenzione e di responsabilità. La sua utilità non risiede nel trasformare un punteggio in un giudizio assoluto, ma nel costringere ogni decisione a lasciare una traccia razionale: quali fonti abbiamo consultato, quali rischi abbiamo accettato, quali dipendenze abbiamo escluso e quali misure abbiamo imposto. Una decisione documentata è più difendibile, più controllabile e più facile da correggere quando lo scenario cambia.

L'edizione annuale è un impegno alla revisione. Leggi, alleanze, proprietà industriali, campagne criminali e capacità militari mutano rapidamente; nessuna valutazione può essere considerata permanente. L'obiettivo è costruire una memoria istituzionale che consenta all'Italia di cooperare senza ingenuità, innovare senza perdere controllo e proteggere dati e infrastrutture senza rinunciare alle opportunità della trasformazione digitale.

Massimiliano Nicolini

Capo progetto - Atlante dell'affidabilità digitale
Fondazione Olivetti Tecnologia e Ricerca

Sintesi esecutiva

Entità analizzate	Media FOTR	Mediana FOTR	Punteggi >= 8	Punteggi < 5
208	5,6	5,7	41	72

La comparazione mostra tre realtà distinte. La prima comprende ordinamenti con infrastrutture mature, regole prevedibili, elevata cooperazione cyber e trasferimenti dei dati relativamente lineari. La seconda riunisce Paesi tecnicamente evoluti ma caratterizzati da dipendenze concentrate, poteri pubblici intrusivi, assenza di adeguatezza UE o divergenze strategiche. La terza include ecosistemi fragili, in conflitto, opachi o fortemente dipendenti, nei quali l'operatore italiano deve limitare l'esposizione, mantenere chiavi e controllo in Italia e predisporre una reale possibilità di interruzione.

Principio guida

Maturità tecnologica e affidabilità digitale non sono sinonimi. Un Paese può essere tecnicamente potentissimo e non offrire condizioni sufficienti per dati italiani sensibili; un piccolo ordinamento può essere giuridicamente vicino ma non avere capacità tecnica o regolatoria adeguata alla scala del progetto.

Scenario tecnologico globale

Intelligenza artificiale, modelli fondazionali e agenti autonomi

L'adozione di modelli generativi e agenti che eseguono azioni rende insufficiente la sola valutazione del luogo in cui è ospitata un'applicazione. Occorre mappare modello, provider, inferenza, addestramento, retrieval, plugin, log, moderazione, accesso umano, catena degli acceleratori e possibilità di trasferire prompt o output. I sistemi usati dalla pubblica amministrazione devono essere valutati anche per spiegabilità, sicurezza del dato, dipendenza da API e capacità di continuare il servizio in caso di indisponibilità geopolitica o commerciale.

Cloud, hyperscaler e sovranità operativa

Il cloud concentra capacità e standardizza i servizi, ma può trasformare un contratto locale in una catena globale. La localizzazione del data center non basta quando gestione, supporto, telemetria, chiavi, backup o subresponsabili restano in Paesi terzi. L'Atlante attribuisce valore a portabilità, interoperabilità, controllo delle chiavi, trasparenza societaria, disponibilità di alternative e possibilità di esercitare audit tecnici e contrattuali.

Reti 5G, 6G, cavi, satelliti LEO e continuità

Le reti mobili avanzate, i cavi sottomarini e le costellazioni satellitari sono infrastrutture geopolitiche. RAN e core possono avere origini differenti; un territorio molto connesso può dipendere da pochi approdi, da un solo Paese di transito o da alimentazione non ridondata. Il passaggio verso 5G standalone, edge computing e integrazione satellite-terra amplia la superficie di attacco e rende necessario separare gestione, orchestrazione, identità e dati di localizzazione.

OT, IoT, energia e infrastrutture fisiche digitalizzate

Veicoli connessi, sistemi di accumulo, reti elettriche, impianti industriali, smart city e dispositivi medici producono telemetria e ricevono aggiornamenti remoti. La sicurezza non può essere ridotta alla privacy: firmware, supply chain, manutenzione, protocolli proprietari e comandi a distanza possono influire sulla continuità di servizi essenziali. Le cooperazioni che integrano energia, mobilità, città e dati devono essere considerate come un unico perimetro di rischio.

Semiconduttori, acceleratori e dipendenze industriali

La produzione di chip richiede progettazione, proprietà intellettuale, macchinari, materiali, foundry, packaging e software EDA distribuiti in più Paesi. L'origine commerciale del prodotto finale può quindi occultare dipendenze decisive. Per gli operatori italiani è necessario valutare second sourcing, ciclo di vita, firmware, componenti obsoleti, sanzioni, controlli all'esportazione e disponibilità di ricambi.

Quantum e crittografia post-quantum

La minaccia harvest now, decrypt later rende attuale la protezione di dati che devono rimanere riservati per molti anni. L'Atlante considera positivamente inventari crittografici, crypto-agility, roadmap post-quantum e capacità di gestire certificati

e chiavi. La presenza di laboratori quantum non dimostra da sola preparazione operativa; servono piani di migrazione, test di interoperabilità e controllo della supply chain crittografica.

Biometria, sorveglianza e identità digitale

Biometria facciale, voce, impronte, DNA, analisi comportamentale e identità digitale possono migliorare servizi e sicurezza, ma creano dataset non revocabili e potenzialmente utilizzabili per controllo sociale o discriminazione. Nei rapporti internazionali devono essere verificati finalità, base giuridica, accuratezza, interoperabilità, accessi pubblici, conservazione, possibilità di contestazione e divieto di riuso.

Minacce cyber, ransomware e operazioni di influenza

Ransomware, attacchi alla supply chain, furto di credenziali, compromissione dei fornitori e manipolazione informativa convergono. Le campagne possono essere criminali, statali o ibride e colpire simultaneamente dati, fiducia e continuità. L'affidabilità di un Paese dipende quindi anche dalla capacità di notificare incidenti, cooperare sulle evidenze, proteggere il dibattito pubblico e garantire rimedi indipendenti.

Quadro normativo internazionale, europeo e italiano

Livello internazionale

Il quadro internazionale è composto da strumenti vincolanti e standard volontari. La Convenzione di Budapest del Consiglio d'Europa resta il principale trattato operativo su criminalità informatica ed evidenza elettronica, integrato dai protocolli aggiuntivi. La Convenzione delle Nazioni Unite contro la criminalità informatica, adottata nel 2024 e aperta alla firma tra il 2025 e il 2026, introduce un quadro universale in fase di consolidamento. Rilevano inoltre controllo delle esportazioni e dual-use, regimi sanzionatori, norme sulle telecomunicazioni ITU, principi OCSE e UNESCO sull'intelligenza artificiale, G7 Hiroshima Process e standard ISO/IEC e NIST. Tali fonti non hanno tutte la stessa forza giuridica: l'Atlante le usa per misurare cooperazione, convergenza e qualità dei controlli.

Livello dell’Unione europea

Per l'operatore italiano il nucleo è formato da GDPR e regole sui trasferimenti internazionali, NIS2, direttiva CER, regolamento DORA per il settore finanziario, Cyber Resilience Act, Data Governance Act, Data Act, AI Act, Digital Services Act, Digital Markets Act, eIDAS 2.0, Cybersecurity Act e disciplina europea sul dual-use. Il regime deve essere letto insieme agli atti di esecuzione, alle decisioni di adeguatezza, alle clausole contrattuali standard, alle binding corporate rules, agli orientamenti EDPB ed ENISA e alle norme settoriali. L'applicazione extraterritoriale di alcuni strumenti significa che un fornitore non europeo può comunque essere soggetto a obblighi UE, ma ciò non elimina la verifica dei poteri di accesso nel Paese terzo. Ai fini di questa revisione, l’AI Act è letto nel testo consolidato al 27 luglio 2026, successivo al regolamento (UE) 2026/1744 sulla semplificazione dell’attuazione delle regole armonizzate in materia di intelligenza artificiale.

Livello nazionale italiano

In Italia il quadro comprende il Codice dell'amministrazione digitale, il Codice privacy coordinato con il GDPR, il d.lgs. 138/2024 di attuazione NIS2, la legge 90/2024 sulla cybersicurezza, la disciplina dell'Agenzia per la cybersicurezza nazionale, il perimetro di sicurezza nazionale cibernetica, la legge 132/2025 sull'intelligenza artificiale, il golden power, il Codice dei contratti pubblici, le regole su segreto, sicurezza nazionale, infrastrutture critiche, conservazione documentale e responsabilità amministrativa. Per tecnologie militari o dual-use si aggiungono autorizzazioni, sanzioni, utilizzatore finale e destinazione d’uso e controlli sulle esportazioni. L'Atlante non sostituisce queste verifiche: serve a stabilire quanto approfondirle e quali condizioni inserire prima del rapporto. La legge 23 settembre 2025, n. 132, in vigore dal 10 ottobre 2025, è considerata come disciplina nazionale di principi e di settore coordinata con il regolamento europeo; l’indicatore-paese non la tratta come regime alternativo, ma come livello italiano complementare.

> **Regola sui trasferimenti**
> Quando il Paese non appartiene al SEE e non beneficia di una decisione di adeguatezza, il trasferimento di dati personali dall'Italia richiede uno strumento del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment e misure supplementari. Anche in presenza di adeguatezza restano obbligatorie sicurezza, minimizzazione, finalità e controllo della subfornitura.

Metodo Celeborn Intelligence e architettura degli indici

Nel presente Atlante, l'espressione Celeborn Intelligence identifica il metodo di ricerca e analisi sviluppato dalla Fondazione Olivetti Tecnologia e Ricerca per raccogliere, ordinare, verificare e interpretare informazioni non classificate provenienti da fonti pubbliche, dataset istituzionali e documenti accessibili. La denominazione non indica una fonte separata, ma l'architettura analitica con cui le evidenze vengono ricondotte a indicatori comparabili, valutazioni nazionali e raccomandazioni operative orientate agli interessi dell'Italia.

La pipeline di ricerca segue cinque aree uniformi: infrastrutture e connettività; intelligenza artificiale e tecnologie emergenti; capitale umano e competenze STEM; supply chain e sovranità tecnologica; cybersecurity, libertà digitale e cooperazione. Le ricerche includono fonti ufficiali internazionali, dataset comparabili, atti normativi, siti governativi, autorità, operatori, pubblicazioni accademiche e stampa qualificata in più lingue. Il testo finale è redatto esclusivamente in italiano. Le informazioni non verificabili o non comparabili sono indicate come n.d. e abbassano la confidenza, senza essere sostituite da presunzioni.

Codice	Dimensione	Peso	Variabili considerate
S1	Maturità infrastrutturale	20%	Internet, banda fissa, 5G, ridondanza, cavi e transiti, elettricità, server sicuri.
S2	IA e tecnologie emergenti	20%	Policy IA, cloud, HPC, IoT, servizi pubblici, ecosistema di sviluppo, quantum e crypto-agility.
S3	Capitale umano e STEM	20%	Capitale umano, alfabetizzazione, diffusione digitale, formazione, attrazione e ritenzione dei talenti.
S4	Indipendenza della supply chain	20%	Diversificazione di hardware, software e cloud, produzione locale, controllo di firmware, assistenza e IP.
S5	Postura di sicurezza cyber	20%	GCI, quadro legale, CERT/CSIRT, organizzazione, capacità, cooperazione, libertà digitale e shutdown.

Il Global Cyber-Reliability Index (GCRI) è la media semplice dei cinque punteggi: GCRI = S1 x 0,20 + S2 x 0,20 + S3 x 0,20 + S4 x 0,20 + S5 x 0,20. Valori pari o superiori a 8 indicano una zona tecnicamente matura; valori tra 5 e 7,9 segnalano capacità utilizzabili ma vulnerabilità; valori inferiori a 5 indicano rischio cyber elevato o dati insufficienti.

L'Indice FOTR di affidabilità digitale è invece centrato sull'Italia. Parte dal GCRI e integra compatibilità giuridica, maturità cyber, trasparenza istituzionale, compatibilità strategica, supply chain e trasferibilità dei dati. La differenza FOTR-GCRI è il correttivo italiano: può ridurre il punteggio di potenze tecnicamente avanzate ma non compatibili con i requisiti italiani, oppure aumentarlo quando cooperazione, regole e garanzie rendono affidabile un ecosistema tecnicamente meno maturo.

Indicatore di compliance con AI Act e legge 132/2025

L'indicatore di compatibilità regolatoria è una metrica di prossimità-paese costruita per l'uso degli operatori italiani. Non afferma che uno Stato, un'impresa o un prodotto siano automaticamente conformi: la conformità giuridica riguarda sempre un operatore, un sistema, un modello, un ruolo nella catena del valore, una finalità e una specifica classe di rischio. La scala segnala invece quanto il contesto normativo, istituzionale e tecnico del Paese faciliti o ostacoli il rispetto degli obblighi europei e italiani.

La componente AI Act UE combina compatibilità giuridica, trasparenza istituzionale, maturità cyber, trasferibilità dei dati, capacità di governo dell'intelligenza artificiale, compatibilità strategica e affidabilità della supply chain. La componente legge 132/2025 attribuisce ulteriore rilievo a centralità umana, sicurezza lungo il ciclo di vita, tutela dei dati, non discriminazione, trasparenza, supervisione, verificabilità, settori sensibili e capacità di mantenere controllo, continuità e rimedi nell'ordinamento italiano.

Per i Paesi dell'Unione europea e dello Spazio economico europeo l'indicatore riconosce la maggiore prossimità del quadro comune, senza attribuire un risultato assoluto. Per i Paesi terzi valuta anche la capacità di un fornitore di sostenere obblighi extraterritoriali, rappresentanza, documentazione, audit, trasparenza e sorveglianza del mercato quando sistemi o output sono destinati all'Unione. Il valore è arrotondato a un decimale e deve essere aggiornato quando mutano leggi, autorità, accordi o catene di fornitura.

LEGENDA - COMPLIANCE AI ACT E LEGGE 132/2025

La scala misura la distanza del contesto nazionale dai requisiti attesi da un operatore italiano; non sostituisce la valutazione del singolo sistema.

8,5-10	7,0-8,4	5,0-6,9	3,0-4,9	0-2,9
ALLINEAMENTO MOLTO ELEVATO	COMPATIBILE CON VERIFICHE	ALLINEAMENTO PARZIALE	DISTANZA ELEVATA	RISCHIO CRITICO

AI ACT UE: prossimità ai requisiti del regolamento europeo. LEGGE 132/2025: compatibilità con principi, settori e cautele dell'ordinamento italiano.

Componente	Peso orientativo	Uso nell'indicatore
Compatibilità giuridica	28% AI Act / 11% legge 132	Prevedibilità delle regole, rimedi, protezione dei dati e recepimento dei principi
Trasparenza istituzionale	18% / 10%	Controllabilità dell'azione pubblica, indipendenza e disponibilità documentale
Maturità cyber	15% / 10%	Sicurezza del ciclo di vita, gestione incidenti, resilienza e capacità di audit
Trasferibilità dei dati	15% AI Act	Possibilità di usare basi legittime, SCC/BCR, misure supplementari e localizzazione controllata
Capacità IA e governance	10% AI Act	Adozione, competenze, infrastrutture, valutazione del rischio e supervisione
Strategia e supply chain	14% AI Act / 24% legge 132	Compatibilità con l'Italia, controllo dei fornitori, accessi remoti, continuità e sovranità operativa

Avvertenza legale. Un punteggio elevato non equivale a marcatura, certificazione o dichiarazione di conformità. Prima dell'uso devono essere verificati: ambito territoriale, ruolo di provider/deployer/importatore/distributore, pratiche vietate, classificazione high-risk, obblighi GPAI, gestione del rischio, qualità dei dati, documentazione, registrazione, supervisione umana, robustezza, cybersecurity, trasparenza, diritti degli interessati e norme settoriali italiane.

Cybercrime: metrica, fonti e impiego nella decisione

La sezione cybercrime utilizza il Global Organized Crime Index 2025 della Global Initiative Against Transnational Organized Crime. L'indice copre i 193 Stati membri delle Nazioni Unite e separa mercati criminali, attori criminali e resilienza. Per le quindici entità dell'Atlante non dotate di una serie nazionale autonoma è usato un proxy regionale ponderato, sempre dichiarato nel profilo e accompagnato da minore confidenza.

Il valore dei reati cyber-dipendenti è avverso: un punteggio alto indica maggiore pervasività stimata del mercato criminale. I valori di resilienza, cooperazione internazionale, norme, capacità delle forze dell'ordine, antiriciclaggio, prevenzione e tutela delle vittime sono invece favorevoli quando elevati. L'indice operativo FOTR-CY combina pressione criminale, struttura degli attori e deficit di resilienza; non sostituisce S5, ma agisce come correttivo prudenziale della matrice dei rischi e dei presidi richiesti.

La lettura evita due errori. Il primo è ritenere sicuro un Paese perché registra pochi incidenti: sottodenuncia, scarsa digitalizzazione e limitata capacità forense possono comprimere la visibilità. Il secondo è penalizzare automaticamente gli ordinamenti trasparenti, nei quali incidenti e procedimenti sono più frequentemente resi pubblici. Per questo il dato viene interpretato insieme a capacità investigativa, cooperazione probatoria, qualità dei rimedi e confidenza Celeborn Intelligence.

Fonti metodologiche: regolamento (UE) 2024/1689 nel testo consolidato al 27 luglio 2026, come modificato dal regolamento (UE) 2026/1744; legge 23 settembre 2025, n. 132; Global Organized Crime Index 2025, dataset, metodologia e soglie GI-TOC.

Qualità e priorità delle fonti

Fonte	Copertura	Uso nell'Atlante	Limite principale
World Bank WDI	Oltre 200 economie	Connettività, elettricità, server sicuri	Indicatori di accesso, non di ridondanza o controllo
UN DESA EGDI 2024	Stati ONU e ampio campione	E-government, capitale umano, telecomunicazioni	Misura maturità pubblica aggregata
ITU GCI 2024	Quasi globale	Impegno cyber su cinque pilastri	Non misura vulnerabilità operative segrete
World Bank GTMI 2025	197 economie	Sistemi pubblici, servizi, partecipazione, abilitatori	Parte dei dati è auto-dichiarata
Oxford Insights 2025	195 governi	Capacità pubblica di utilizzare e governare l'IA	Non equivale a capacità di calcolo sovrana

Fonte	Copertura	Uso nell'Atlante	Limite principale
Freedom on the Net 2025	72 Paesi, 87% utenti globali	Censura, accesso, diritti degli utenti	Non copre tutte le entità
Freedom in the World 2026	208 Paesi e territori	Controlli, libertà e prevedibilità istituzionale	Non è un indice di cybersicurezza
Commissione europea	Paesi terzi rilevanti	Adeguatezza e strumenti di trasferimento	Le decisioni possono essere riesaminate
Consiglio d'Europa	Parti e invitati	Cooperazione su cybercrime ed evidenza elettronica	Ratifica non prova attuazione effettiva

Come leggere le tabelle dei capitoli nazionali

Dashboard del Paese

Mostra posizione nel ranking, status, area, FOTR, GCRI, classe operativa, confidenza Celeborn Intelligence e regime dei dati. È la vista di valutazione preliminare, non la decisione finale.

Indicatori Celeborn Intelligence comparabili

Raccoglie valori e anno delle fonti globali. La colonna "uso" indica quale parte dell'algoritmo alimentano. I dati mancanti riducono confidenza e richiedono verifica locale.

Scorecard GCRI S1-S5

Confronta le cinque dimensioni tecniche con peso identico. Serve a capire se la debolezza dipende da reti, IA, persone, supply chain o sicurezza.

Componenti FOTR

Trasformano la capacità tecnica in affidabilità per l'Italia. Compatibilità giuridica e trasferibilità dati possono produrre un risultato diverso dal GCRI.

Matrice dei rischi

Applica la valutazione a sei categorie: dati personali, sanità/biometria, cloud/infrastrutture, IP/R&S, PA, difesa/dual-use. Orienta autorizzazioni, segregazione e controlli.

Presidi e decisione operativa

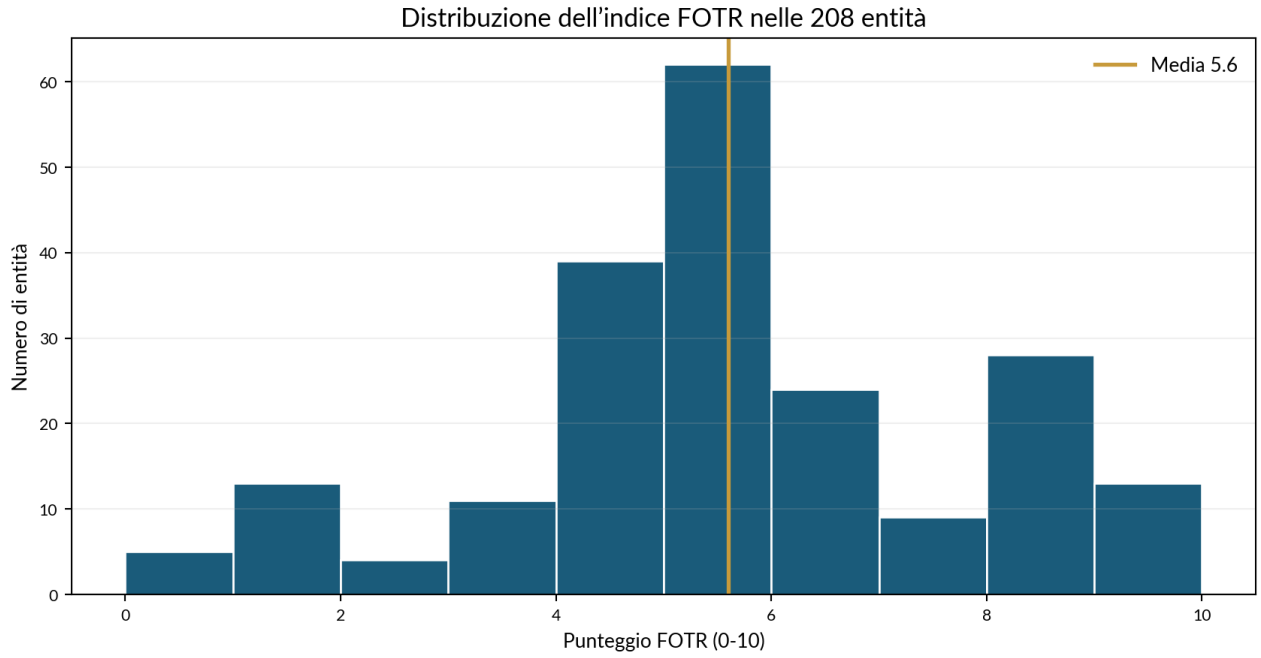
Indicano condizioni minime per iniziare, mantenere o interrompere la cooperazione. Devono essere trasposte in capitolati, contratti, architetture e piani di uscita.

Limiti e cautele interpretative

L'Atlante non valuta capacità offensive classificate, vulnerabilità operative o informazioni ottenute con metodi intrusivi.
Le medie nazionali non sostituiscono l'analisi del singolo ente, impresa, data center, prodotto o contratto.
La trasparenza può aumentare il numero di incidenti pubblici; il silenzio informativo non prova assenza di attacchi.
Un accordo internazionale o la ratifica di un trattato non garantiscono attuazione, indipendenza dell'autorità o rimedi effettivi.
Le entità de facto e i territori sono inclusi per utilità operativa; la denominazione non esprime riconoscimento politico.
Il punteggio è datato e deve essere riesaminato prima di decisioni rilevanti o dopo eventi geopolitici e normativi significativi.

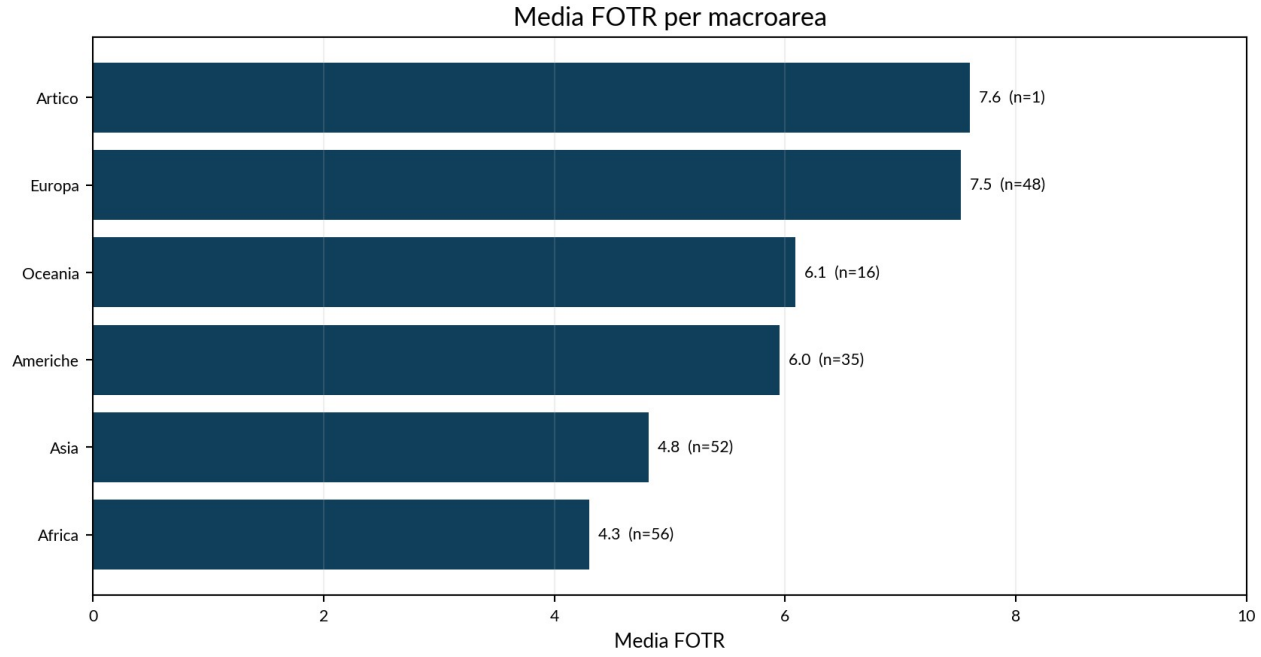
Quadro comparativo e ranking

Distribuzione dei punteggi



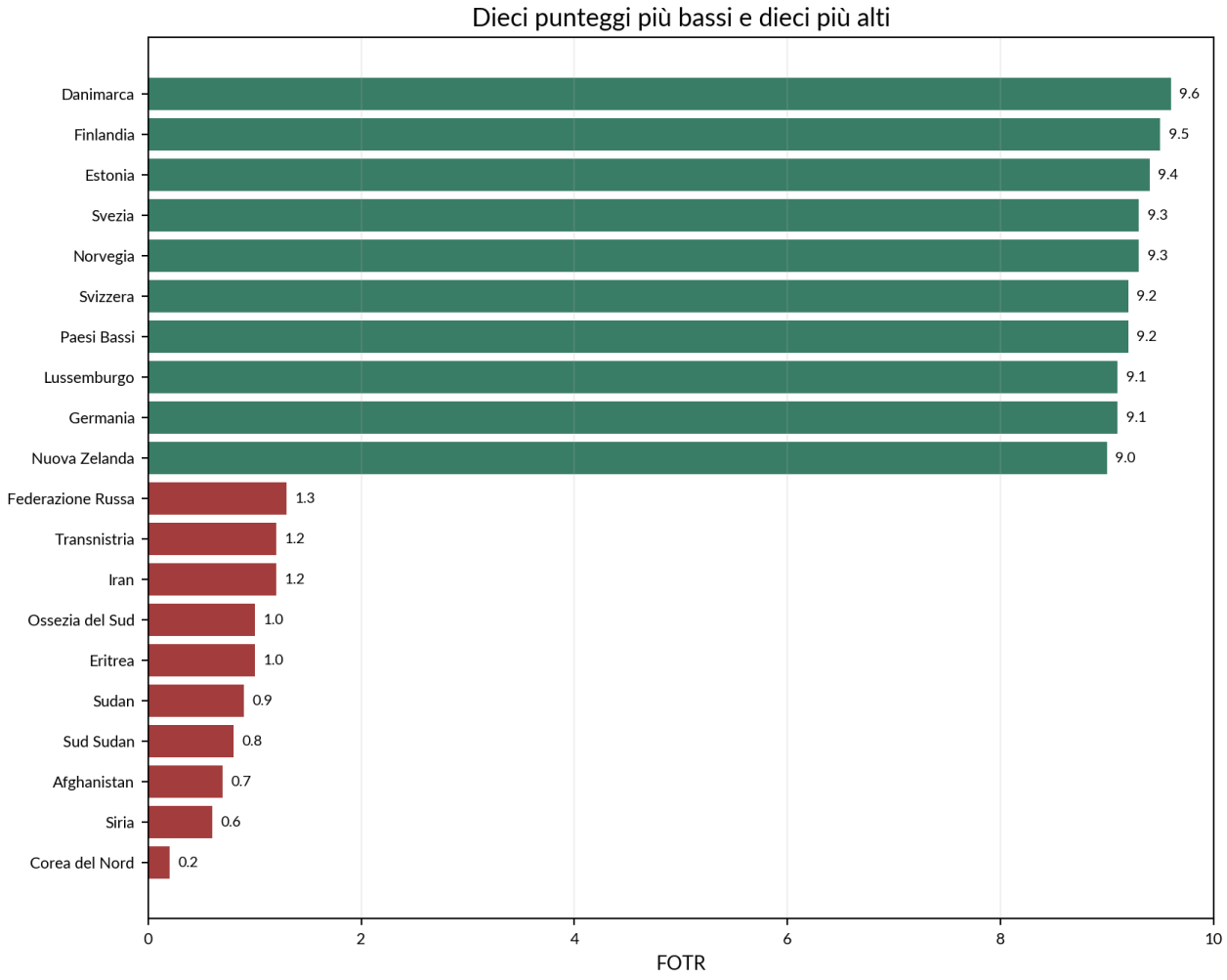
Elaborazione FOTR su 208 profili. La linea indica la media dell'edizione 2026.

Confronto per macroarea



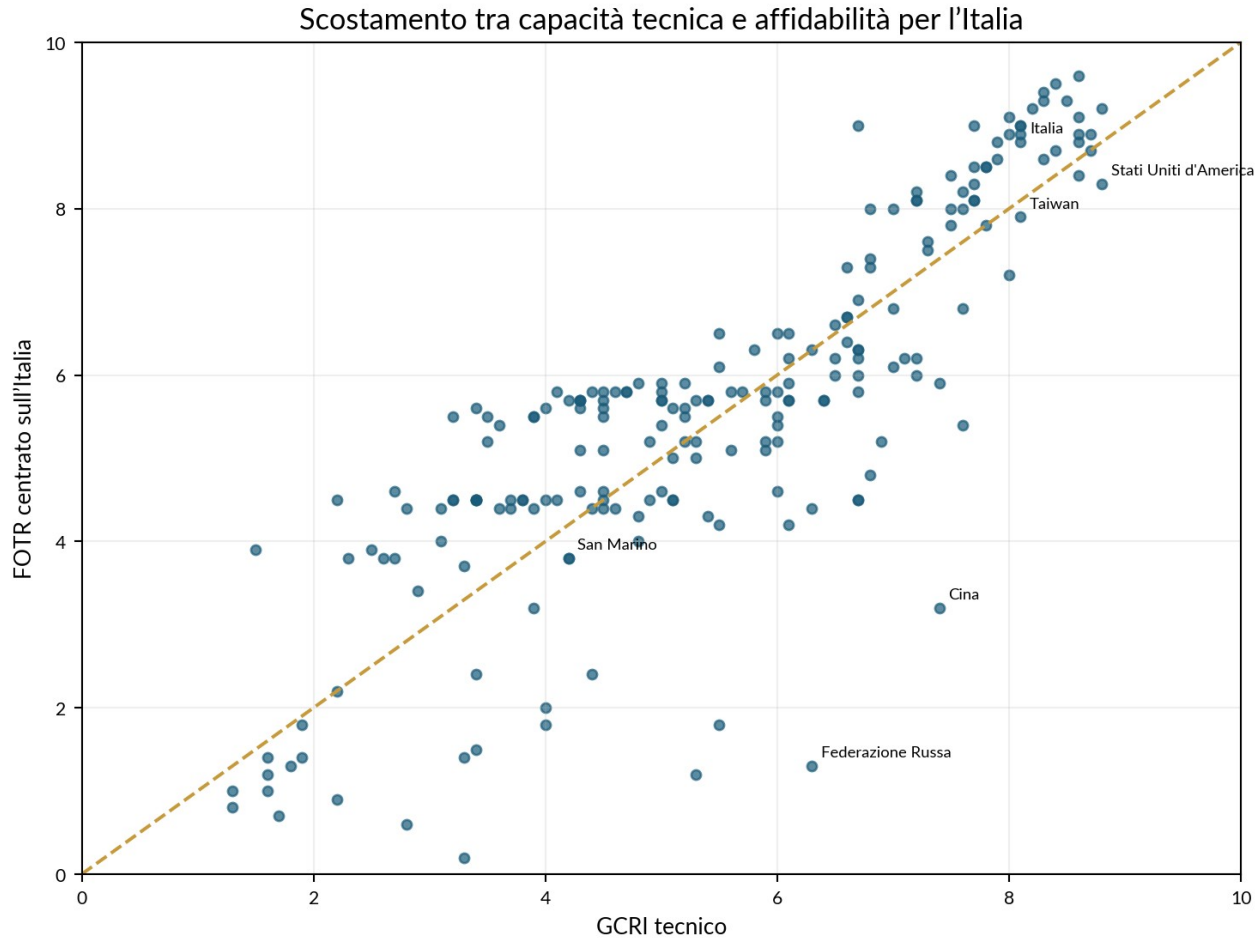
Media semplice dei punteggi FOTR; le dimensioni dei gruppi non sono identiche.

Estremi del ranking



Il grafico mostra le code della distribuzione; non costituisce una graduatoria politica generale.

GCRI e correttivo italiano



I punti sotto la diagonale hanno un FOTR inferiore alla maturità tecnica; quelli sopra beneficiano di prossimità normativa o strategica.

Ranking generale FOTR

Pos.	Paese o entità	Area	FOTR	GCRI	Classe	Confidenza
1	**Danimarca**	Europa	9,6	8,6	Affidabilità molto alta	Alta
2	**Finlandia**	Europa	9,5	8,4	Affidabilità molto alta	Alta
3	**Estonia**	Europa	9,4	8,3	Affidabilità molto alta	Alta
4	**Norvegia**	Europa	9,3	8,5	Affidabilità molto alta	Alta
5	**Svezia**	Europa	9,3	8,3	Affidabilità molto alta	Alta
6	**Paesi Bassi**	Europa	9,2	8,8	Affidabilità molto alta	Alta
7	**Svizzera**	Europa	9,2	8,2	Affidabilità molto alta	Alta
8	**Germania**	Europa	9,1	8,6	Affidabilità molto alta	Alta
9	**Lussemburgo**	Europa	9,1	8,0	Affidabilità molto alta	Alta
10	**Canada**	Americhe	9,0	8,1	Affidabilità molto alta	Alta
11	**Islanda**	Europa	9,0	8,1	Affidabilità molto alta	Alta
12	**Liechtenstein**	Europa	9,0	6,7	Affidabilità molto alta	Alta
13	**Nuova Zelanda**	Oceania	9,0	7,7	Affidabilità molto alta	Alta
14	**Australia**	Oceania	8,9	8,7	Affidabilità alta	Alta
15	**Austria**	Europa	8,9	8,0	Affidabilità alta	Alta
16	**Francia**	Europa	8,9	8,6	Affidabilità alta	Alta

Pos.	Paese o entità	Area	FOTR	GCRI	Classe	Confidenza
17	**Irlanda**	Europa	8,9	8,1	Affidabilità alta	Alta
18	**Belgio**	Europa	8,8	7,9	Affidabilità alta	Alta
19	**Giappone**	Asia	8,8	8,6	Affidabilità alta	Alta
20	**Italia**	Europa	8,8	8,1	Affidabilità alta	Alta
21	**Corea del Sud**	Asia	8,7	8,7	Affidabilità alta	Alta
22	**Regno Unito**	Europa	8,7	8,4	Affidabilità alta	Alta
23	**Portogallo**	Europa	8,6	7,9	Affidabilità alta	Alta
24	**Spagna**	Europa	8,6	8,3	Affidabilità alta	Alta
25	**Cechia**	Europa	8,5	7,7	Affidabilità alta	Alta
26	**Lituania**	Europa	8,5	7,8	Affidabilità alta	Alta
27	**Slovenia**	Europa	8,5	7,8	Affidabilità alta	Alta
28	**Lettonia**	Europa	8,4	7,5	Affidabilità alta	Alta
29	**Singapore**	Asia	8,4	8,6	Affidabilità alta	Alta
30	**Malta**	Europa	8,3	7,7	Affidabilità alta	Alta
31	**Stati Uniti d'America**	Americhe	8,3	8,8	Affidabilità alta	Alta
32	**Polonia**	Europa	8,2	7,6	Affidabilità alta	Alta
33	**Slovacchia**	Europa	8,2	7,2	Affidabilità alta	Alta
34	**Cipro**	Europa	8,1	7,7	Affidabilità alta	Alta
35	**Croazia**	Europa	8,1	7,2	Affidabilità alta	Alta
36	**Grecia**	Europa	8,1	7,7	Affidabilità alta	Alta
37	**Romania**	Europa	8,1	7,2	Affidabilità alta	Alta
38	**Bulgaria**	Europa	8,0	7,0	Affidabilità alta	Alta
39	**Santa Sede / Stato della Città del Vaticano**	Europa	8,0	6,8	Affidabilità alta	Bassa
40	**Ungheria**	Europa	8,0	7,5	Affidabilità alta	Alta
41	**Uruguay**	Americhe	8,0	7,6	Affidabilità alta	Alta
42	**Taiwan**	Asia	7,9	8,1	Affidabilità favorevole ma condizionata	Bassa
43	**Brasile**	Americhe	7,8	7,5	Affidabilità favorevole ma condizionata	Alta
44	**Israele**	Asia	7,8	7,8	Affidabilità favorevole ma condizionata	Alta
45	**Groenlandia**	Artico	7,6	7,3	Affidabilità favorevole ma condizionata	Media
46	**Cile**	Americhe	7,5	7,3	Affidabilità favorevole ma condizionata	Alta
47	**Argentina**	Americhe	7,4	6,8	Affidabilità favorevole ma condizionata	Alta
48	**Andorra**	Europa	7,3	6,6	Affidabilità favorevole ma condizionata	Alta

Pos.	Paese o entità	Area	FOTR	GCRI	Classe	Confidenza
49	**Costa Rica**	Americhe	7,3	6,8	Affidabilità favorevole ma condizionata	Alta
50	**Emirati Arabi Uniti**	Asia	7,2	8,0	Affidabilità favorevole ma condizionata	Alta
51	**Monaco**	Europa	6,9	6,7	Affidabilità favorevole ma condizionata	Alta
52	**Malaysia**	Asia	6,8	7,6	Affidabilità favorevole ma condizionata	Alta
53	**Mauritius**	Africa	6,8	7,0	Affidabilità favorevole ma condizionata	Alta
54	**Messico**	Americhe	6,7	6,6	Affidabilità favorevole ma condizionata	Alta
55	**Ucraina**	Europa	6,7	6,6	Affidabilità favorevole ma condizionata	Alta
56	**Colombia**	Americhe	6,6	6,5	Affidabilità favorevole ma condizionata	Alta
57	**Isole Cook**	Oceania	6,5	6,1	Affidabilità favorevole ma condizionata	Bassa
58	**Panama**	Americhe	6,5	6,0	Affidabilità favorevole ma condizionata	Alta
59	**Seychelles**	Africa	6,5	5,5	Affidabilità favorevole ma condizionata	Alta
60	**Sudafrica**	Africa	6,4	6,6	Affidabilità selettiva	Alta
61	**Georgia**	Asia	6,3	6,7	Affidabilità selettiva	Alta
62	**Montenegro**	Europa	6,3	6,3	Affidabilità selettiva	Alta
63	**Niue**	Oceania	6,3	5,8	Affidabilità selettiva	Bassa
64	**Perù**	Americhe	6,3	6,7	Affidabilità selettiva	Alta
65	**India**	Asia	6,2	6,7	Affidabilità selettiva	Alta
66	**Macedonia del Nord**	Europa	6,2	6,1	Affidabilità selettiva	Alta
67	**Moldova**	Europa	6,2	6,5	Affidabilità selettiva	Alta
68	**Qatar**	Asia	6,2	7,1	Affidabilità selettiva	Alta
69	**Thailandia**	Asia	6,2	7,2	Affidabilità selettiva	Alta
70	**Botswana**	Africa	6,1	5,5	Affidabilità selettiva	Alta
71	**Oman**	Asia	6,1	7,0	Affidabilità selettiva	Alta
72	**Albania**	Europa	6,0	6,7	Affidabilità selettiva	Alta
73	**Bahrein**	Asia	6,0	7,2	Affidabilità selettiva	Alta
74	**Filippine**	Asia	6,0	6,5	Affidabilità selettiva	Alta
75	**Belize**	Americhe	5,9	5,0	Affidabilità selettiva	Media
76	**El Salvador**	Americhe	5,9	5,2	Affidabilità selettiva	Alta
77	**Guyana**	Americhe	5,9	4,8	Affidabilità selettiva	Alta

Pos.	Paese o entità	Area	FOTR	GCRI	Classe	Confidenza
78	Repubblica Dominicana	Americhe	5,9	6,1	Affidabilità selettiva	Alta
79	Serbia	Europa	5,9	7,4	Affidabilità selettiva	Alta
80	Antigua e Barbuda	Americhe	5,8	4,4	Affidabilità selettiva	Alta
81	Barbados	Americhe	5,8	5,0	Affidabilità selettiva	Alta
82	Ghana	Africa	5,8	5,9	Affidabilità selettiva	Alta
83	Giamaica	Americhe	5,8	5,6	Affidabilità selettiva	Alta
84	Grenada	Americhe	5,8	4,5	Affidabilità selettiva	Alta
85	Guatemala	Americhe	5,8	4,6	Affidabilità selettiva	Alta
86	Indonesia	Asia	5,8	6,7	Affidabilità selettiva	Alta
87	Kenya	Africa	5,8	5,7	Affidabilità selettiva	Alta
88	Kuwait	Asia	5,8	6,0	Affidabilità selettiva	Alta
89	Namibia	Africa	5,8	4,7	Affidabilità selettiva	Alta
90	Nicaragua	Americhe	5,8	4,1	Affidabilità selettiva	Alta
91	Suriname	Americhe	5,8	4,7	Affidabilità selettiva	Alta
92	Armenia	Asia	5,7	6,1	Affidabilità selettiva	Alta
93	Bahamas	Americhe	5,7	5,3	Affidabilità selettiva	Alta
94	Bolivia	Americhe	5,7	5,0	Affidabilità selettiva	Alta
95	Dominica	Americhe	5,7	4,3	Affidabilità selettiva	Alta
96	Ecuador	Americhe	5,7	6,4	Affidabilità selettiva	Alta
97	Giordania	Asia	5,7	6,4	Affidabilità selettiva	Alta
98	Honduras	Americhe	5,7	4,3	Affidabilità selettiva	Alta
99	Kiribati	Oceania	5,7	4,3	Affidabilità selettiva	Alta
100	Marocco	Africa	5,7	6,1	Affidabilità selettiva	Alta
101	Paraguay	Americhe	5,7	5,9	Affidabilità selettiva	Alta
102	Ruanda	Africa	5,7	5,4	Affidabilità selettiva	Alta
103	Saint Kitts e Nevis	Americhe	5,7	5,0	Affidabilità selettiva	Alta
104	Saint Vincent e Grenadine	Americhe	5,7	4,5	Affidabilità selettiva	Alta
105	Tonga	Oceania	5,7	4,2	Affidabilità selettiva	Alta
106	Trinidad e Tobago	Americhe	5,7	5,4	Affidabilità selettiva	Alta
107	Bosnia ed Erzegovina	Europa	5,6	5,2	Affidabilità selettiva	Alta
108	Figi	Oceania	5,6	5,1	Affidabilità selettiva	Alta
109	Micronesia	Oceania	5,6	3,4	Affidabilità selettiva	Media
110	Saint Lucia	Americhe	5,6	4,3	Affidabilità selettiva	Alta
111	Samoa	Oceania	5,6	4,0	Affidabilità selettiva	Alta
112	Vanuatu	Oceania	5,6	4,5	Affidabilità selettiva	Alta
113	Isole Salomone	Oceania	5,5	3,2	Affidabilità selettiva	Alta
114	Kosovo	Europa	5,5	5,2	Affidabilità selettiva	Bassa
115	Nauru	Oceania	5,5	3,9	Affidabilità selettiva	Alta
116	Palau	Oceania	5,5	4,5	Affidabilità selettiva	Alta
117	Papua Nuova Guinea	Oceania	5,5	3,9	Affidabilità selettiva	Alta

Pos.	Paese o entità	Area	FOTR	GCRI	Classe	Confidenza
118	Tunisia	Africa	5,5	6,0	Affidabilità selettiva	Alta
119	Tuvalu	Oceania	5,5	3,5	Affidabilità selettiva	Alta
120	Arabia Saudita	Asia	5,4	7,6	Affidabilità selettiva	Alta
121	Isole Marshall	Oceania	5,4	3,6	Affidabilità selettiva	Alta
122	Mongolia	Asia	5,4	6,0	Affidabilità selettiva	Alta
123	Senegal	Africa	5,4	5,0	Affidabilità selettiva	Alta
124	Bangladesh	Asia	5,2	5,9	Affidabilità selettiva	Alta
125	Brunei	Asia	5,2	6,0	Affidabilità selettiva	Alta
126	Cambogia	Asia	5,2	4,9	Affidabilità selettiva	Alta
127	Costa d'Avorio	Africa	5,2	5,2	Affidabilità selettiva	Alta
128	Nepal	Asia	5,2	5,3	Affidabilità selettiva	Alta
129	Timor-Leste	Asia	5,2	3,5	Affidabilità selettiva	Alta
130	Turchia	Asia	5,2	6,9	Affidabilità selettiva	Alta
131	Bhutan	Asia	5,1	5,6	Affidabilità selettiva	Alta
132	Laos	Asia	5,1	4,3	Affidabilità selettiva	Alta
133	Maldive	Asia	5,1	4,5	Affidabilità selettiva	Alta
134	Sri Lanka	Asia	5,1	5,9	Affidabilità selettiva	Alta
135	Nigeria	Africa	5,0	5,3	Affidabilità selettiva	Alta
136	Pakistan	Asia	5,0	5,1	Affidabilità selettiva	Alta
137	Kazakistan	Asia	4,8	6,8	Rischio alto	Alta
138	Eswatini	Africa	4,6	5,0	Rischio alto	Alta
139	Guinea-Bissau	Africa	4,6	2,7	Rischio alto	Alta
140	Hong Kong (RAS)	Asia	4,6	6,0	Rischio alto	Media
141	Iraq	Asia	4,6	4,3	Rischio alto	Alta
142	Libano	Asia	4,6	4,5	Rischio alto	Alta
143	Angola	Africa	4,5	4,0	Rischio alto	Alta
144	Benin	Africa	4,5	4,9	Rischio alto	Alta
145	Comore	Africa	4,5	3,2	Rischio alto	Alta
146	Gambia	Africa	4,5	3,8	Rischio alto	Alta
147	Gibuti	Africa	4,5	3,4	Rischio alto	Alta
148	Lesotho	Africa	4,5	3,8	Rischio alto	Alta
149	Madagascar	Africa	4,5	3,2	Rischio alto	Alta
150	Mauritania	Africa	4,5	3,7	Rischio alto	Alta
151	Repubblica del Congo	Africa	4,5	3,4	Rischio alto	Alta
152	Sierra Leone	Africa	4,5	3,4	Rischio alto	Alta
153	São Tomé e Príncipe	Africa	4,5	3,4	Rischio alto	Alta
154	Tanzania	Africa	4,5	5,1	Rischio alto	Alta
155	Uganda	Africa	4,5	4,5	Rischio alto	Alta
156	Uzbekistan	Asia	4,5	6,7	Rischio alto	Alta
157	Vietnam	Asia	4,5	6,7	Rischio alto	Alta

Pos.	Paese o entità	Area	FOTR	GCRI	Classe	Confidenza
158	Yemen	Asia	4,5	2,2	Rischio alto	Alta
159	Zambia	Africa	4,5	5,1	Rischio alto	Alta
160	Zimbabwe	Africa	4,5	4,1	Rischio alto	Alta
161	Azerbaigian	Asia	4,4	6,3	Rischio alto	Alta
162	Camerun	Africa	4,4	4,4	Rischio alto	Alta
163	Gabon	Africa	4,4	4,5	Rischio alto	Alta
164	Guinea	Africa	4,4	3,7	Rischio alto	Alta
165	Guinea Equatoriale	Africa	4,4	3,1	Rischio alto	Alta
166	Liberia	Africa	4,4	2,8	Rischio alto	Alta
167	Malawi	Africa	4,4	3,9	Rischio alto	Alta
168	Mozambico	Africa	4,4	3,6	Rischio alto	Alta
169	Togo	Africa	4,4	4,6	Rischio alto	Alta
170	Algeria	Africa	4,3	5,4	Rischio alto	Alta
171	Capo Verde	Africa	4,3	4,8	Rischio alto	Alta
172	Egitto	Africa	4,2	6,1	Rischio alto	Alta
173	Kirghizistan	Asia	4,2	5,5	Rischio alto	Alta
174	Macao (RAS)	Asia	4,0	4,8	Rischio alto	Media
175	Repubblica Democratica del Congo	Africa	4,0	3,1	Rischio alto	Alta
176	Burundi	Africa	3,9	2,5	Rischio alto	Alta
177	Repubblica Centrafricana	Africa	3,9	1,5	Rischio alto	Alta
178	Ciad	Africa	3,8	2,6	Rischio alto	Alta
179	Etiopia	Africa	3,8	4,2	Rischio alto	Alta
180	Mali	Africa	3,8	2,7	Rischio alto	Alta
181	Niger	Africa	3,8	2,3	Rischio alto	Alta
182	San Marino	Europa	3,8	4,2	Rischio alto	Alta
183	Burkina Faso	Africa	3,7	3,3	Rischio alto	Alta
184	Cipro del Nord	Europa	3,4	2,9	Rischio estremo	Bassa
185	Cina	Asia	3,2	7,4	Rischio estremo	Alta
186	Tagikistan	Asia	3,2	3,9	Rischio estremo	Alta
187	Cuba	Americhe	2,4	4,4	Rischio estremo	Alta
188	Palestina	Asia	2,4	3,4	Rischio estremo	Media
189	Somaliland	Africa	2,2	2,2	Rischio estremo	Bassa
190	Venezuela	Americhe	2,0	4,0	Rischio estremo	Alta
191	Bielorussia	Europa	1,8	5,5	Rischio estremo	Alta
192	Libia	Africa	1,8	4,0	Rischio estremo	Alta
193	Sahara Occidentale / RASD	Africa	1,8	1,9	Rischio estremo	Bassa
194	Myanmar	Asia	1,5	3,4	Rischio estremo	Alta
195	Abkhazia	Asia	1,4	1,6	Rischio estremo	Bassa
196	Haiti	Americhe	1,4	1,9	Rischio estremo	Alta

Pos.	Paese o entità	Area	FOTR	GCRI	Classe	Confidenza
197	**Turkmenistan**	Asia	1,4	3,3	Rischio estremo	Alta
198	**Federazione Russa**	Europa	1,3	6,3	Rischio estremo	Alta
199	**Somalia**	Africa	1,3	1,8	Rischio estremo	Alta
200	**Iran**	Asia	1,2	5,3	Rischio estremo	Alta
201	**Transnistria**	Europa	1,2	1,6	Rischio estremo	Bassa
202	**Eritrea**	Africa	1,0	1,6	Rischio estremo	Alta
203	**Ossezia del Sud**	Asia	1,0	1,3	Rischio estremo	Bassa
204	**Sudan**	Africa	0,9	2,2	Rischio estremo	Alta
205	**Sud Sudan**	Africa	0,8	1,3	Rischio estremo	Alta
206	**Afghanistan**	Asia	0,7	1,7	Rischio estremo	Alta
207	**Siria**	Asia	0,6	2,8	Rischio estremo	Alta
208	**Corea del Nord**	Asia	0,2	3,3	Rischio estremo	Media

Indice alfabetico delle 208 entità

A - D	E - L	M - S	T - Z
Abkhazia - 1,4	El Salvador - 5,9	Liberia - 4,4	Ruanda - 5,7
Afghanistan - 0,7	Emirati Arabi Uniti - 7,2	Libia - 1,8	Sahara Occidentale / RASD - 1,8
Albania - 6,0	Eritrea - 1,0	Liechtenstein - 9,0	Saint Kitts e Nevis - 5,7
Algeria - 4,3	Estonia - 9,4	Lituania - 8,5	Saint Lucia - 5,6
Andorra - 7,3	Eswatini - 4,6	Lussemburgo - 9,1	Saint Vincent e Grenadine - 5,7
Angola - 4,5	Etiopia - 3,8	Macao (RAS) - 4,0	Samoa - 5,6
Antigua e Barbuda - 5,8	Federazione Russa - 1,3	Macedonia del Nord - 6,2	San Marino - 3,8
Arabia Saudita - 5,4	Figi - 5,6	Madagascar - 4,5	Santa Sede / Stato della Città del Vaticano - 8,0
Argentina - 7,4	Filippine - 6,0	Malawi - 4,4	Senegal - 5,4
Armenia - 5,7	Finlandia - 9,5	Malaysia - 6,8	Serbia - 5,9
Australia - 8,9	Francia - 8,9	Maldive - 5,1	Seychelles - 6,5
Austria - 8,9	Gabon - 4,4	Mali - 3,8	Sierra Leone - 4,5
Azerbaigian - 4,4	Gambia - 4,5	Malta - 8,3	Singapore - 8,4
Bahamas - 5,7	Georgia - 6,3	Marocco - 5,7	Siria - 0,6
Bahrein - 6,0	Germania - 9,1	Mauritania - 4,5	Slovacchia - 8,2
Bangladesh - 5,2	Ghana - 5,8	Mauritius - 6,8	Slovenia - 8,5
Barbados - 5,8	Giamaica - 5,8	Messico - 6,7	Somalia - 1,3
Belgio - 8,8	Giappone - 8,8	Micronesia - 5,6	Somaliland - 2,2
Belize - 5,9	Gibuti - 4,5	Moldova - 6,2	Spagna - 8,6
Benin - 4,5	Giordania - 5,7	Monaco - 6,9	Sri Lanka - 5,1
Bhutan - 5,1	Grecia - 8,1	Mongolia - 5,4	Stati Uniti d'America - 8,3
Bielorussia - 1,8	Grenada - 5,8	Montenegro - 6,3	Sud Sudan - 0,8
Bolivia - 5,7	Groenlandia - 7,6	Mozambico - 4,4	Sudafrica - 6,4
Bosnia ed Erzegovina - 5,6	Guatemala - 5,8	Myanmar - 1,5	Sudan - 0,9
Botswana - 6,1	Guinea - 4,4	Namibia - 5,8	Suriname - 5,8
Brasile - 7,8	Guinea Equatoriale - 4,4	Nauru - 5,5	Svezia - 9,3
Brunei - 5,2	Guinea-Bissau - 4,6	Nepal - 5,2	Svizzera - 9,2
Bulgaria - 8,0	Guyana - 5,9	Nicaragua - 5,8	São Tomé e Príncipe - 4,5
Burkina Faso - 3,7	Haiti - 1,4	Niger - 3,8	Tagikistan - 3,2

A - D	E - L	M - S	T - Z
Burundi - 3,9	Honduras - 5,7	Nigeria - 5,0	Taiwan - 7,9
Cambogia - 5,2	Hong Kong (RAS) - 4,6	Niue - 6,3	Tanzania - 4,5
Camerun - 4,4	India - 6,2	Norvegia - 9,3	Thailandia - 6,2
Canada - 9,0	Indonesia - 5,8	Nuova Zelanda - 9,0	Timor-Leste - 5,2
Capo Verde - 4,3	Iran - 1,2	Oman - 6,1	Togo - 4,4
Cechia - 8,5	Iraq - 4,6	Ossezia del Sud - 1,0	Tonga - 5,7
Ciad - 3,8	Irlanda - 8,9	Paesi Bassi - 9,2	Transnistria - 1,2
Cile - 7,5	Islanda - 9,0	Pakistan - 5,0	Trinidad e Tobago - 5,7
Cina - 3,2	Isole Cook - 6,5	Palau - 5,5	Tunisia - 5,5
Cipro - 8,1	Isole Marshall - 5,4	Palestina - 2,4	Turchia - 5,2
Cipro del Nord - 3,4	Isole Salomone - 5,5	Panama - 6,5	Turkmenistan - 1,4
Colombia - 6,6	Israele - 7,8	Papua Nuova Guinea - 5,5	Tuvalu - 5,5
Comore - 4,5	Italia - 8,8	Paraguay - 5,7	Ucraina - 6,7
Corea del Nord - 0,2	Kazakistan - 4,8	Perù - 6,3	Uganda - 4,5
Corea del Sud - 8,7	Kenya - 5,8	Polonia - 8,2	Ungheria - 8,0
Costa Rica - 7,3	Kirghizistan - 4,2	Portogallo - 8,6	Uruguay - 8,0
Costa d'Avorio - 5,2	Kiribati - 5,7	Qatar - 6,2	Uzbekistan - 4,5
Croazia - 8,1	Kosovo - 5,5	Regno Unito - 8,7	Vanuatu - 5,6
Cuba - 2,4	Kuwait - 5,8	Repubblica Centrafricana - 3,9	Venezuela - 2,0
Danimarca - 9,6	Laos - 5,1	Repubblica Democratica del Congo - 4,0	Vietnam - 4,5
Dominica - 5,7	Lesotho - 4,5	Repubblica Dominicana - 5,9	Yemen - 4,5
Ecuador - 5,7	Lettonia - 8,4	Repubblica del Congo - 4,5	Zambia - 4,5
Egitto - 4,2	Libano - 4,6	Romania - 8,1	Zimbabwe - 4,5

Profili nazionali ed entità analizzate

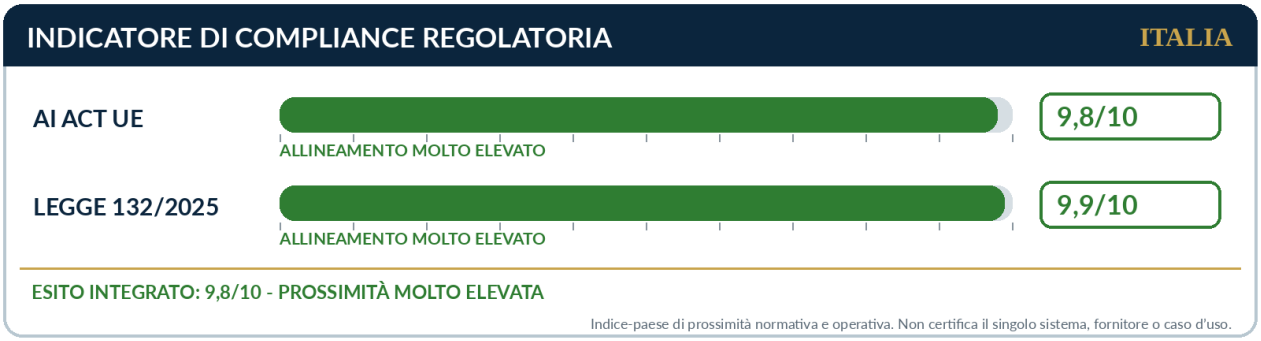
I capitoli seguenti sono ordinati con l'Italia in apertura e, successivamente, in ordine alfabetico. Ogni profilo usa la medesima architettura per consentire confronti, ma la parte descrittiva è specifica per contesto, dati e posizione geopolitica. I valori sono espressi con una cifra decimale; n.d. indica assenza di evidenza sufficientemente comparabile alla data di chiusura.

Chiusura editoriale: 5 agosto 2026. Le fonti nazionali e internazionali sono richiamate nel singolo profilo e nella bibliografia finale.

Italia

Posizione FOTR	20	Area	Europa	Subregione	Europa meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	8,8	GCRI / 10	8,1	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Italia, AI Act UE 9,8/10; legge 132/2025 9,9/10; esito integrato 9,8/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

L'Italia costituisce il centro prospettico dell'Atlante e non un Paese valutato come gli altri. La sua posizione nel mercato unico, nell'Unione europea, nella NATO e nelle catene industriali mediterranee impone di distinguere la disponibilità commerciale di una tecnologia dalla sua effettiva controllabilità giuridica, operativa e strategica. La base industriale nazionale convive con dipendenze significative da hyperscaler statunitensi, componentistica asiatica e filiere globali dei semiconduttori. Per questo l'indice italiano è anche il riferimento rispetto al quale vengono misurate trasferibilità dei dati, compatibilità delle regole, continuità dei servizi e possibilità di sostituire il fornitore. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 87/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,1/10) e indice FOTR (8,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Paese pivot dell'Atlante: mercato UE, infrastrutture critiche nazionali, amministrazioni pubbliche, filiere industriali e capacità di difesa devono essere protetti con una lettura integrata di diritto, geopolitica e supply chain.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	89,2% / 31,8 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 30.647 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	83,6 / 84,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	100,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	70,5/100 - rank 25	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	74/100 - Libero / Libero (87/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,0 / 6,4 / 5,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Italia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Italia le evidenze principali sono GTMI 84,2/100, EGDI 83,6/100, GCI 100,0/100, AI readiness 70,5/100. La dimensione più robusta è maturità infrastrutturale (8,9/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (7,3/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Italia è 8,9/10. La base statistica rileva utenti Internet pari al 89,2% nel 2024; 31,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 30.647 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Italia al posto 25 con un valore medio di 70,5/100; il pilastro migliore è governance (85,8/100), quello più debole è sviluppo e diffusione (61,4/100). Il GTMI 2025 è 84,2/100. Il punteggio S2 è 7,3/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Italia è valutata sufficiente ma disomogenea, con S3 pari a 7,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 84,3/100, sviluppo e diffusione dell'IA 61,4/100, penetrazione Internet 89,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Italia ottiene S4 7,6/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 7,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Italia, Fornitori nazionali ed europei, con forte presenza statunitense nel cloud, nel software e nella cybersicurezza; componentistica asiatica nelle reti e nell'hardware. L'impatto sulla valutazione è misurato

da S4=7,6/10 e dal proxy di indipendenza 7,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Italia è S5 8,9/10. La base ITU registra ITU GCI 100,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure giuridiche (20,0/20). Freedom on the Net è 74/100 - Libero, mentre Freedom in the World è Libero (87/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR e Codice privacy (d.lgs. 196/2003, come modificato); d.lgs. 138/2024 di attuazione NIS2; legge 90/2024 sulla cybersicurezza; perimetro di sicurezza nazionale cibernetica; disciplina ACN; legge 132/2025 sull'intelligenza artificiale, coordinata con l'AI Act.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,0	Crimini finanziari	7,0
Reti criminali	4,0	Attori incorporati nello Stato	7,0
Attori stranieri	7,5	Attori del settore privato	7,0
Resilienza complessiva	6,4	Cooperazione internazionale	9,0
Politiche e norme nazionali	7,5	Forze dell'ordine	8,0
Antiriciclaggio	5,5	Prevenzione	6,0
Supporto vittime e testimoni	5,5	Rischio operativo FOTR-CY	5,6 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Italia il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,6/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 6,0/10; le frodi e i reati finanziari 7,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (7,5/10) e attori incorporati nello Stato (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Italia assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Italia, la resilienza complessiva è intermedia (6,4/10); la cooperazione internazionale è robusta (9,0/10), le politiche e norme nazionali sono robuste (7,5/10) e la capacità delle forze dell'ordine è robusta (8,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 5,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Italia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Italia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Italia, In Italia le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La disponibilità

del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Italia, L'amministrazione italiana utilizza identità digitale, pagamenti pubblici, interoperabilità, cloud qualificato e piattaforme nazionali. La priorità è consolidare inventari, classificazione dei dati, NIS2, continuità, sicurezza della supply chain e capacità di controllo sovrano delle chiavi.

Tecnologie militari e dual-use. Per Italia, Sul piano militare e dual-use, Italia mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Italia, GDPR e Codice privacy (d.lgs. 196/2003, come modificato); d.lgs. 138/2024 di attuazione NIS2; legge 90/2024 sulla cybersicurezza; perimetro di sicurezza nazionale cibernetica; disciplina ACN; legge 132/2025 sull'intelligenza artificiale, coordinata con l'AI Act. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Italia, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,7/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,9	7,3	7,8	7,6	8,9	8,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,5	8,1	8,0	9,2	8,3	9,7

Il GCRI di Italia è 8,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,7/10), mentre il più basso è Trasparenza istituzionale (8,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Medio-basso	Basso	Medio-basso	Basso

La matrice applica il FOTR di 8,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Italia, la cautela si concentra su 2 ambiti a rischio intermedio: Cloud e infrastrutture, Pubblica amministrazione. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Italia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Italia, L'Italia è il punto di riferimento dell'intero indice. La postura raccomandata combina autonomia decisionale, interoperabilità UE/NATO, protezione delle infrastrutture critiche, valutazione degli investimenti esteri, qualificazione cloud, cifratura, controllo delle chiavi e capacità di sostituzione del fornitore.

Decisione operativa indicativa. Per Italia, il FOTR di 8,8/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (8,0/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

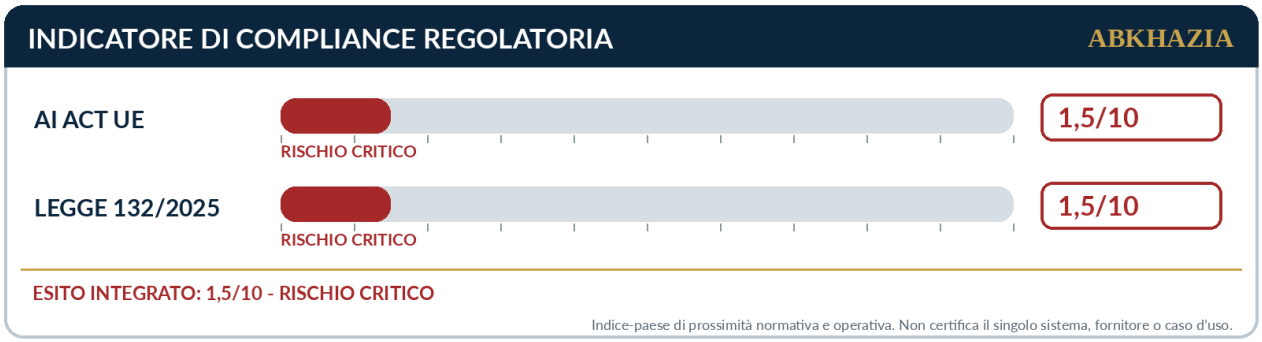
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Italia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Abkhazia

Posizione FOTR	195	Area	Asia	Subregione	Caucaso
Status	Entità de facto a riconoscimento limitato	Confidenza Celeborn Intelligence	Bassa	Copertura dati	0/7 famiglie
FOTR / 10	1,4	GCRI / 10	1,6	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Abkhazia, AI Act UE 1,5/10; legge 132/2025 1,5/10; esito integrato 1,5/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Nel quadro di Asia, Abkhazia presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Russia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 40/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (1,6/10) e indice FOTR (1,4/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Ambiente de facto dipendente dalla Federazione Russa, con riconoscimento limitato, scarsa trasparenza e assenza di rimedi internazionalmente affidabili.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	n.d. / n.d. per 100	n.d./n.d.	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	n.d. / n.d. per milione	n.d./n.d.	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	n.d. / n.d.	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	n.d./100 - n.d.	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	n.d./100 - rank n.d.	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (40/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,2 / 4,1 / 6,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Abkhazia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 0/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Abkhazia le evidenze principali sono nessun indicatore composito pienamente comparabile. La dimensione più robusta è maturità infrastrutturale (2,2/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (0,1/10). Sono disponibili 0 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata bassa. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Abkhazia è 2,2/10. La base statistica rileva i principali dati WDI non sono disponibili in forma omogenea. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Per Abkhazia non è disponibile un profilo Oxford Insights direttamente attribuibile; l'adozione di IA è quindi valutata attraverso GovTech, servizi online, infrastrutture e fonti qualitative. Il punteggio S2 è 1,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Abkhazia è valutata fragile, con S3 pari a 0,1/10. Le evidenze disponibili comprendono evidenza quantitativa incompleta. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Abkhazia ottiene S4 1,8/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Russia; l'indicatore di indipendenza disponibile è 1,8/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Abkhazia, Dipendenza quasi totale da reti, operatori e fornitori russi. L'impatto sulla valutazione è misurato da S4=1,8/10 e dal proxy di indipendenza 1,8/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Abkhazia è S5 1,8/10. La base ITU registra GCI non disponibile in forma comparabile. Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (40/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,2	Crimini finanziari	7,2
Reti criminali	5,4	Attori incorporati nello Stato	6,8
Attori stranieri	4,1	Attori del settore privato	6,9
Resilienza complessiva	4,1	Cooperazione internazionale	3,9
Politiche e norme nazionali	6,0	Forze dell'ordine	5,1
Antiriciclaggio	4,0	Prevenzione	4,1
Supporto vittime e testimoni	4,3	Rischio operativo FOTR-CY	6,7 - ALTO

Sintesi del rischio cybercrime. Abkhazia presenta un'esposizione stimata alta (6,7/10): reati cyber-dipendenti 7,2/10, crimini finanziari 7,2/10 e resilienza 4,1/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori del settore privato (6,9/10) e attori incorporati nello Stato (6,8/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Abkhazia assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Abkhazia, la resilienza complessiva è debole (4,1/10); la cooperazione internazionale è debole (3,9/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è debole (5,1/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 4,1/10 e supporto a vittime e testimoni 4,3/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Abkhazia, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; blocco di hosting e ASN ad alta reputazione negativa, ricerca proattiva delle minacce su malware sottrattori di informazioni e controllo dei canali RDP/VPN; verifica indipendente della proprietà e dei subfornitori. Poiché l'entità non dispone di una serie nazionale GI-TOC autonoma, i valori derivano da un proxy Celeborn Intelligence ponderato su Georgia 45%, Federazione Russa 55%; la confidenza deve pertanto essere considerata inferiore e la decisione resa più prudente.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; proxy Celeborn Intelligence ponderato su Georgia 45%, Federazione Russa 55%. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Abkhazia, In Abkhazia le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. Per

i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Abkhazia, Il livello governativo di Abkhazia presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Abkhazia, Sul piano militare e dual-use, Abkhazia mostra forte integrazione o dipendenza dall'ecosistema russo, inclusi sistemi di comando, comunicazione e sicurezza. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Abkhazia, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Abkhazia, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 0,0/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
2,2	1,9	0,1	1,8	1,8	1,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
2,5	2,8	0,1	0,6	1,9	0,0

Il GCRI di Abkhazia è 1,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 1,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Maturità cyber (2,8/10), mentre il più basso è Trasferibilità dati (0,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 1,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Abkhazia, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Abkhazia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Abkhazia, Dal punto di vista italiano, Abkhazia rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Abkhazia, il FOTR di 1,4/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

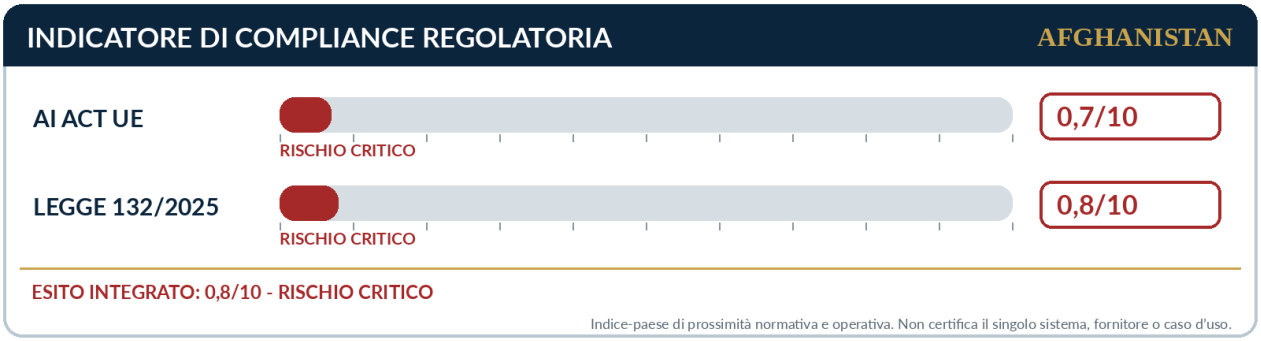
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Abkhazia: World Development Indicators, valori più recenti disponibili 2022-2024; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Bassa con copertura 0/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Afghanistan

Posizione FOTR	206	Area	Asia	Subregione	Asia meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	0,7	GCRI / 10	1,7	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Afghanistan, AI Act UE 0,7/10; legge 132/2025 0,8/10; esito integrato 0,8/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Afghanistan, situato in Asia meridionale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 8/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (1,7/10) è superiore al punteggio FOTR (0,7/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Il rapporto digitale con Afghanistan deve essere considerato eccezionale e ad alta esposizione. Sono necessari screening sanzionatori, autorizzazioni, segregazione completa e impossibilità tecnica di accedere ai dati in chiaro.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	16,1% / 0,1 per 100	2024/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	87,8% / 41 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	20,8 / 12,1	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	18,4/100 - Tier 5 - capacità iniziali	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	15,3/100 - rank 188	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (8/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,0 / 1,5 / 7,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Afghanistan, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Afghanistan le evidenze principali sono GTMI 12,1/100, EGDI 20,8/100, GCI 18,4/100, AI readiness 15,3/100. La dimensione più robusta è indipendenza della supply chain (2,7/10), mentre la criticità relativa riguarda postura di sicurezza cyber (0,7/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Afghanistan è 2,1/10. La base statistica rileva utenti Internet pari al 16,1% nel 2024; 0,1 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 87,8% nel 2024; 41 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Afghanistan al posto 188 con un valore medio di 15,3/100; il pilastro migliore è adozione pubblica (26,8/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 12,1/100. Il punteggio S2 è 1,5/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Afghanistan è valutata fragile, con S3 pari a 1,7/10. Le evidenze disponibili comprendono indice UN di capitale umano 26,4/100, sviluppo e diffusione dell'IA 11,8/100, penetrazione Internet 16,1%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Afghanistan ottiene S4 2,7/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Afghanistan, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo

societario e subfornitura. L'impatto sulla valutazione è misurato da S4=2,7/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Afghanistan è S5 0,7/10. La base ITU registra ITU GCI 18,4/100, Tier 5 - capacità iniziali; il pilastro relativamente più debole è cooperazione (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (8/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo non stabile, forti controlli sull'informazione, sanzioni e assenza di rimedi affidabili; trasferimenti di dati sensibili o strategici da escludere.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,0	Crimini finanziari	8,0
Reti criminali	8,0	Attori incorporati nello Stato	9,0
Attori stranieri	6,0	Attori del settore privato	8,0
Resilienza complessiva	1,5	Cooperazione internazionale	1,5
Politiche e norme nazionali	1,5	Forze dell'ordine	1,5
Antiriciclaggio	1,0	Prevenzione	1,0
Supporto vittime e testimoni	1,0	Rischio operativo FOTR-CY	7,0 - ALTO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (4,0/10), criminalità finanziaria (8,0/10) e resilienza (1,5/10) colloca Afghanistan in una fascia di rischio alto, pari a 7,0/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e reti criminali (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Afghanistan assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Afghanistan, la resilienza complessiva è molto debole (1,5/10); la cooperazione internazionale è molto debole (1,5/10), le politiche e norme nazionali sono molto deboli (1,5/10) e la capacità delle forze dell'ordine è molto debole (1,5/10). Completano il quadro antiriciclaggio 1,0/10, prevenzione 1,0/10 e supporto a vittime e testimoni 1,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Afghanistan, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Afghanistan. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Afghanistan, In Afghanistan le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture

esterne. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Afghanistan, Il livello governativo di Afghanistan presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Afghanistan, Sul piano militare e dual-use, Afghanistan mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Afghanistan, Quadro normativo non stabile, forti controlli sull'informazione, sanzioni e assenza di rimedi affidabili; trasferimenti di dati sensibili o strategici da escludere. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Afghanistan, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 0,0/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
2,1	1,5	1,7	2,7	0,7	1,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
0,9	1,3	0,0	0,9	1,3	0,0

Il GCRI di Afghanistan è 1,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 0,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (1,3/10), mentre il più basso è Trasparenza istituzionale (0,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 0,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Afghanistan, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Afghanistan, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Afghanistan, Dal punto di vista italiano, Afghanistan rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Afghanistan, il FOTR di 0,7/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

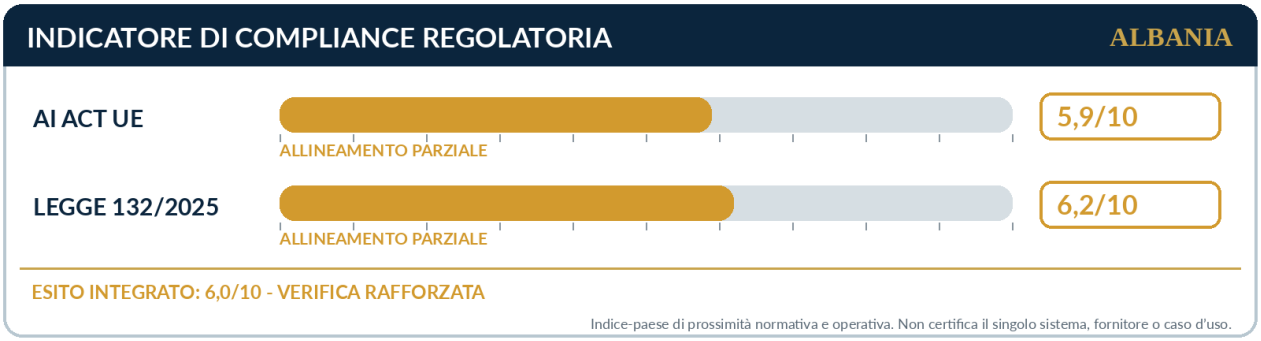
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Afghanistan: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Albania

Posizione FOTR	72	Area	Europa	Subregione	Europa sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	6,0	GCRI / 10	6,7	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Albania, AI Act UE 5,9/10; legge 132/2025 6,2/10; esito integrato 6,0/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Albania non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La collocazione nell'Alleanza Atlantica favorisce interoperabilità e cooperazione di sicurezza, senza equivalere automaticamente ad allineamento pieno sul diritto dei dati. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Cina, Russia, Turchia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 69/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,7/10) e indice FOTR (6,0/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il quadro di Albania è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	85,9% / 24,9 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 1.513 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	80,0 / 93,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	86,5/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	43,5/100 - rank 85	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (69/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 5,2 / 5,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Albania, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Albania le evidenze principali sono GTMI 93,9/100, EGDI 80,0/100, GCI 86,5/100, AI readiness 43,5/100. La dimensione più robusta è maturità infrastrutturale (7,8/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (5,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Albania è 7,8/10. La base statistica rileva utenti Internet pari al 85,9% nel 2024; 24,9 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 1.513 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Albania al posto 85 con un valore medio di 43,5/100; il pilastro migliore è adozione pubblica (69,0/100), quello più debole è politiche pubbliche (23,0/100). Il GTMI 2025 è 93,9/100. Il punteggio S2 è 5,9/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Albania è valutata sufficiente ma disomogenea, con S3 pari a 5,9/10. Le evidenze disponibili comprendono indice UN di capitale umano 81,1/100, sviluppo e diffusione dell'IA 24,4/100, penetrazione Internet 85,9%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Albania ottiene S4 6,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Cina, Russia, Turchia; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Albania, Mercato multi-fornitore tra Unione europea, Stati Uniti, Turchia, Cina e, in alcuni segmenti, Russia; il peso relativo varia tra pubblico, telecomunicazioni e difesa. L'impatto sulla valutazione è

misurato da S4=6,1/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Albania è S5 7,6/10. La base ITU registra ITU GCI 86,5/100, Tier 2 - avanzato; il pilastro relativamente più debole è sviluppo delle capacità (12,1/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (69/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Quadro nazionale di protezione dati e cybersicurezza in progressivo allineamento all'acquis dell'Unione europea; la distanza tra legge formale, vigilanza e prassi deve essere verificata nel settore interessato.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	6,0
Reti criminali	7,0	Attori incorporati nello Stato	6,5
Attori stranieri	3,0	Attori del settore privato	4,5
Resilienza complessiva	5,2	Cooperazione internazionale	7,0
Politiche e norme nazionali	6,0	Forze dell'ordine	5,5
Antiriciclaggio	4,5	Prevenzione	5,0
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	5,4 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Albania il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,4/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 5,5/10; le frodi e i reati finanziari 6,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (7,0/10) e attori incorporati nello Stato (6,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Albania assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Albania, la resilienza complessiva è debole (5,2/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 5,0/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Albania, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Albania. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Albania, In Albania le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Albania, Il livello governativo di Albania presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Albania, Sul piano militare e dual-use, Albania mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Albania, Quadro nazionale di protezione dati e cybersicurezza in progressivo allineamento all'acquis dell'Unione europea; la distanza tra legge formale, vigilanza e prassi deve essere verificata nel settore interessato. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Albania, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,4/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,8	5,9	5,9	6,1	7,6	6,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,0	6,0	5,3	8,3	5,1	5,4

Il GCRI di Albania è 6,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (8,3/10), mentre il più basso è Supply chain (5,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Albania, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Albania, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Albania, Dal punto di vista italiano, Albania rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Albania è indicata una cooperazione selettiva, coerente con il FOTR di 6,0/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Supply chain a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

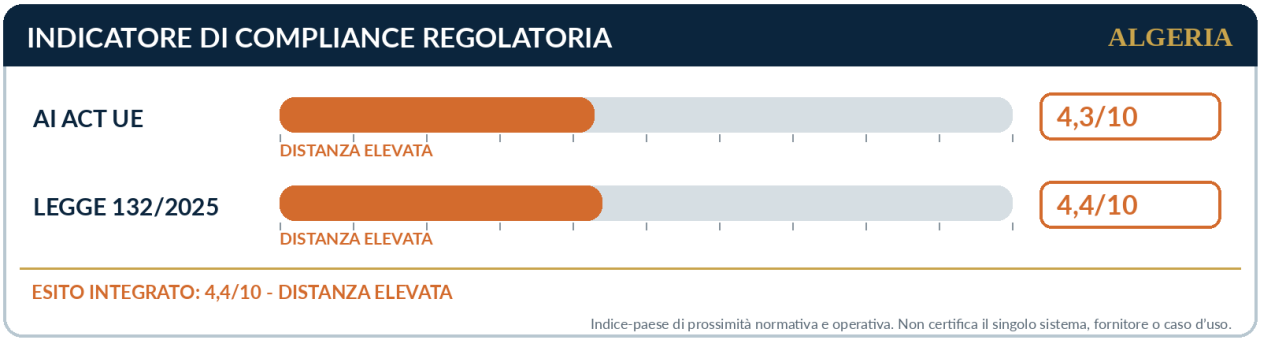
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Albania: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Algeria

Posizione FOTR	170	Area	Africa	Subregione	Africa settentrionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,3	GCRI / 10	5,4	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Algeria, AI Act UE 4,3/10; legge 132/2025 4,4/10; esito integrato 4,4/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Algeria è stato membro delle nazioni unite collocato in Africa settentrionale. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Cina, Russia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 31/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (5,4/10) è superiore al punteggio FOTR (4,3/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Algeria è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	77,4% / 13,3 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 119 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	59,6 / 55,5	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	65,9/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	43,7/100 - rank 89	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (31/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 4,2 / 5,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Algeria, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Algeria le evidenze principali sono GTMI 55,5/100, EGDI 59,6/100, GCI 65,9/100, AI readiness 43,7/100. La dimensione più robusta è maturità infrastrutturale (6,9/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,5/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Algeria è 6,9/10. La base statistica rileva utenti Internet pari al 77,4% nel 2024; 13,3 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 119 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Algeria al posto 89 con un valore medio di 43,7/100; il pilastro migliore è politiche pubbliche (65,5/100), quello più debole è adozione pubblica (26,4/100). Il GTMI 2025 è 55,5/100. Il punteggio S2 è 4,5/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Algeria è valutata sufficiente ma disomogenea, con S3 pari a 5,3/10. Le evidenze disponibili comprendono indice UN di capitale umano 64,2/100, sviluppo e diffusione dell'IA 33,9/100, penetrazione Internet 77,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Algeria ottiene S4 4,7/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Cina, Russia; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Algeria, Forte presenza cinese, europea e russa, con priorità a controllo e localizzazione statale. L'impatto sulla valutazione è misurato da S4=4,7/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Algeria è S5 5,8/10. La base ITU registra ITU GCI 65,9/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (8,6/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (31/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Legge 18-07 sulla protezione dei dati e regole di localizzazione/telecomunicazioni; trasferimenti soggetti a vincoli e autorizzazioni.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	8,0
Reti criminali	5,0	Attori incorporati nello Stato	7,5
Attori stranieri	5,0	Attori del settore privato	4,5
Resilienza complessiva	4,2	Cooperazione internazionale	5,0
Politiche e norme nazionali	6,5	Forze dell'ordine	6,0
Antiriciclaggio	4,0	Prevenzione	3,5
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	5,7 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Algeria il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,7/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 4,5/10; le frodi e i reati finanziari 8,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,5/10) e reti criminali (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Algeria assumono particolare rilevanza phishing e credential theft, ransomware, frodi d'investimento, attacchi a energia e servizi pubblici, abuso di cripto-attività e campagne che possono combinare profitto, spionaggio e pressione politica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Algeria, la resilienza complessiva è debole (4,2/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è intermedia (6,0/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 3,5/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Algeria, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Algeria. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Algeria, In Algeria le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità

del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Algeria, Il livello governativo di Algeria presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Algeria, Sul piano militare e dual-use, Algeria mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Algeria, Legge 18-07 sulla protezione dei dati e regole di localizzazione/telecomunicazioni; trasferimenti soggetti a vincoli e autorizzazioni. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Algeria, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 3,9/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,9	4,5	5,3	4,7	5,8	5,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,4	4,3	4,2	5,1	3,9	3,9

Il GCRI di Algeria è 5,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,3/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,1/10), mentre il più basso è Supply chain (3,9/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,3/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Algeria, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Algeria, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Algeria, Dal punto di vista italiano, Algeria rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Algeria ricade nella fascia di alto rischio (4,3/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

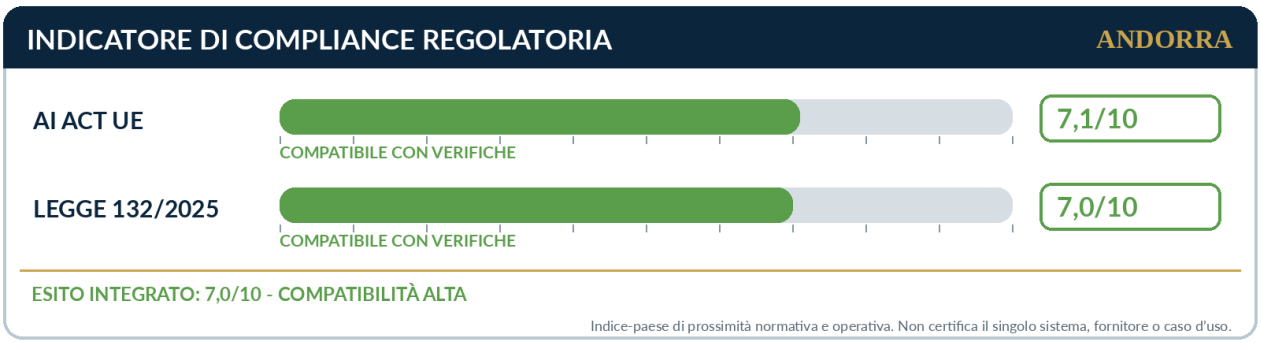
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Algeria: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Andorra

Posizione FOTR	48	**Area**	Europa	**Subregione**	Europa occidentale e centrale
Status	Stato membro delle Nazioni Unite	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	7,3	**GCRI / 10**	6,6	**Classe operativa**	**Affidabilità favorevole ma condizionata**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Andorra, AI Act UE 7,1/10; legge 132/2025 7,0/10; esito integrato 7,0/10, classe «Compatibile con verifiche». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Prima dell'ingaggio occorre una analisi degli scostamenti mirata su trasparenza, governance dei dati, rappresentanza nell'UE, audit e rimedi contrattuali.

Premessa geopolitica e tecnologica

Nel quadro di Europa, Andorra presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La prossimità europea può ridurre i costi operativi, ma non sostituisce la verifica dell'allineamento al GDPR, delle autorità indipendenti e della reale origine dei servizi cloud. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, Russia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 93/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,6/10) e indice FOTR (7,3/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ambiente digitale di Andorra è complessivamente affidabile e aperto agli scambi. Per investimenti italiani è opportuno verificare la disciplina locale, la struttura dei fornitori e gli eventuali poteri pubblici di accesso.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	94,4% / 52,4 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 17.623 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	68,9 / 39,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	76,7/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	41,1/100 - rank 92	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (93/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 8,0 / 2,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Andorra, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Andorra le evidenze principali sono GTMI 39,0/100, EGDI 68,9/100, GCI 76,7/100, AI readiness 41,1/100. La dimensione più robusta è maturità infrastrutturale (9,4/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,2/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Andorra è 9,4/10. La base statistica rileva utenti Internet pari al 94,4% nel 2024; 52,4 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 17.623 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Andorra al posto 92 con un valore medio di 41,1/100; il pilastro migliore è governance (54,3/100), quello più debole è adozione pubblica (25,8/100). Il GTMI 2025 è 39,0/100. Il punteggio S2 è 4,2/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Andorra è valutata sufficiente ma disomogenea, con S3 pari a 5,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 66,7/100, sviluppo e diffusione dell'IA 37,7/100, penetrazione Internet 94,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Andorra ottiene S4 6,0/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, Russia; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Andorra, Ecosistema multi-fornitore con dipendenze europee, statunitensi, russe o cinesi da verificare per singolo settore e livello di governo. L'impatto sulla valutazione è misurato da S4=6,0/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Andorra è S5 7,4/10. La base ITU registra ITU GCI 76,7/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (11,7/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (93/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Disciplina nazionale della protezione dei dati, delle comunicazioni elettroniche e dei reati informatici, con differenze rispetto al GDPR; trasferimenti e accessi pubblici richiedono una verifica locale aggiornata.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	5,5
Reti criminali	3,5	Attori incorporati nello Stato	1,0
Attori stranieri	5,5	Attori del settore privato	5,0
Resilienza complessiva	8,0	Cooperazione internazionale	8,5
Politiche e norme nazionali	8,5	Forze dell'ordine	8,5
Antiriciclaggio	7,5	Prevenzione	8,5
Supporto vittime e testimoni	8,5	Rischio operativo FOTR-CY	2,9 - CONTENUTO

Quadro criminale digitale. Per Andorra, l'indice operativo FOTR-CY è 2,9/10, classe contenuta. Il mercato dei reati cyber-dipendenti è limitato o poco osservabile (2,0/10), mentre i crimini finanziari sono elevati (5,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (5,5/10) e attori del settore privato (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Andorra assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Andorra, la resilienza complessiva è robusta (8,0/10); la cooperazione internazionale è robusta (8,5/10), le politiche e norme nazionali sono robuste (8,5/10) e la capacità delle forze dell'ordine è robusta (8,5/10). Completano il quadro antiriciclaggio 7,5/10, prevenzione 8,5/10 e supporto a vittime e testimoni 8,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Andorra, il livello contenuto non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Andorra. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Andorra, In Andorra le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Andorra, Il livello governativo di Andorra presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Andorra, Sul piano militare e dual-use, Andorra mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Andorra, Disciplina nazionale della protezione dei dati, delle comunicazioni elettroniche e dei reati informatici, con differenze rispetto al GDPR; trasferimenti e accessi pubblici richiedono una verifica locale aggiornata. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Andorra, È disponibile una decisione UE di adeguatezza. L'operatore italiano deve comunque controllare la portata della decisione, i trasferimenti successivi, le misure di sicurezza e le eventuali discipline settoriali. La componente FOTR di trasferibilità è 8,6/10 e il rischio sui dati personali è Medio-basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,4	4,2	5,8	6,0	7,4	6,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
7,6	6,9	6,9	6,9	6,5	8,6

Il GCRI di Andorra è 6,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 7,3/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (8,6/10), mentre il più basso è Supply chain (6,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-basso	Medio-basso	Medio	Medio-basso	Medio	Medio

La matrice applica il FOTR di 7,3/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Andorra, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Andorra, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Andorra, Dal punto di vista italiano, Andorra rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Andorra è favorevole ma condizionata: il valore FOTR di 7,3/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Supply chain.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

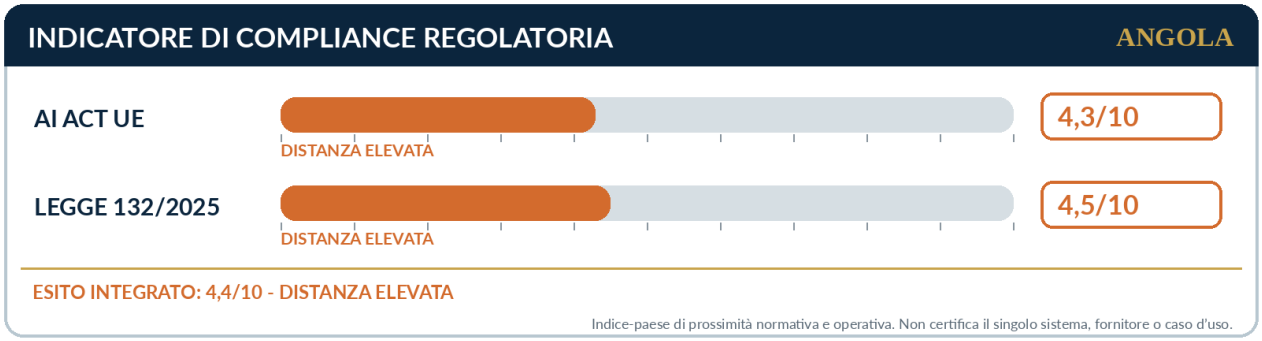
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Andorra: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Angola

Posizione FOTR	143	Area	Africa	Subregione	Africa australe
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	4,5	GCRI / 10	4,0	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Angola, AI Act UE 4,3/10; legge 132/2025 4,5/10; esito integrato 4,4/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Angola, situato in Africa australe, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 28/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (4,0/10) e indice FOTR (4,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per Angola non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	40,7% / 0,4 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	55,5% / 49 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	41,5 / 59,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	39,5/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	27,1/100 - rank 141	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	60/100 - Parzialmente libero / Non libero (28/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 4,2 / 5,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Angola, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Angola le evidenze principali sono GTMI 59,3/100, EGDI 41,5/100, GCI 39,5/100, AI readiness 27,1/100. La dimensione più robusta è indipendenza della supply chain (4,7/10), mentre la criticità relativa riguarda maturità infrastrutturale (3,3/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Angola è 3,3/10. La base statistica rileva utenti Internet pari al 40,7% nel 2024; 0,4 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 55,5% nel 2024; 49 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Angola al posto 141 con un valore medio di 27,1/100; il pilastro migliore è governance (53,0/100), quello più debole è sviluppo e diffusione (14,1/100). Il GTMI 2025 è 59,3/100. Il punteggio S2 è 3,5/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Angola è valutata fragile, con S3 pari a 4,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 47,6/100, sviluppo e diffusione dell'IA 14,1/100, penetrazione Internet 40,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Angola ottiene S4 4,7/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Angola, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,7/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Angola è S5 4,5/10. La base ITU registra ITU GCI 39,5/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (1,8/20). Freedom on the Net è 60/100 - Parzialmente libero, mentre Freedom in the World è Non libero (28/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	6,0
Reti criminali	6,0	Attori incorporati nello Stato	8,0
Attori stranieri	5,5	Attori del settore privato	7,5
Resilienza complessiva	4,2	Cooperazione internazionale	5,0
Politiche e norme nazionali	5,0	Forze dell'ordine	4,0
Antiriciclaggio	4,5	Prevenzione	4,0
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	5,9 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Angola il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,9/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 5,5/10; le frodi e i reati finanziari 6,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e attori del settore privato (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Angola assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Angola, la resilienza complessiva è debole (4,2/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 4,0/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Angola, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Angola. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Angola, In Angola le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità

del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Angola, Il livello governativo di Angola presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Angola, Sul piano militare e dual-use, Angola mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Angola, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Angola, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,2/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,3	3,5	4,0	4,7	4,5	4,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,4	4,3	4,3	5,2	4,5	4,2

Il GCRI di Angola è 4,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,2/10), mentre il più basso è Trasferibilità dati (4,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Angola, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Angola, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Angola, Dal punto di vista italiano, Angola rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Angola ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

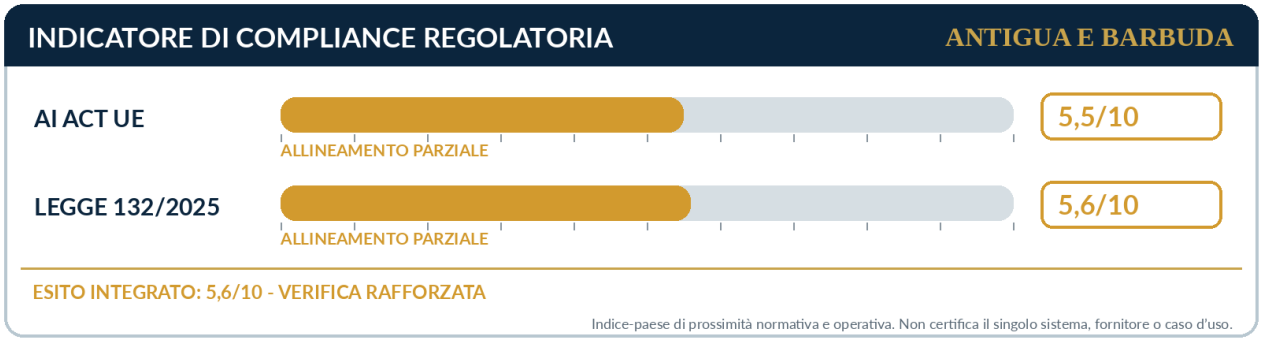
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Angola: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Antigua e Barbuda

Posizione FOTR	80	Area	Americhe	Subregione	Caraibi
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,8	GCRI / 10	4,4	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Antigua e Barbuda, AI Act UE 5,5/10; legge 132/2025 5,6/10; esito integrato 5,6/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Antigua e Barbuda non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 83/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,8/10) supera il GCRI tecnico (4,4/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Antigua e Barbuda dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	72,7% / 10,7 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 970 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	64,3 / 19,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	18,2/100 - Tier 5 - capacità iniziali	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	25,4/100 - rank 147	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (83/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Firmatario/invitato	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	1,5 / 4,7 / 3,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Antigua e Barbuda, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Antigua e Barbuda le evidenze principali sono GTMI 19,4/100, EGDI 64,3/100, GCI 18,2/100, AI readiness 25,4/100. La dimensione più robusta è maturità infrastrutturale (6,8/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,7/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Antigua e Barbuda è 6,8/10. La base statistica rileva utenti Internet pari al 72,7% nel 2024; 10,7 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 100,0% nel 2024; 970 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Antigua e Barbuda al posto 147 con un valore medio di 25,4/100; il pilastro migliore è governance (48,4/100), quello più debole è sviluppo e diffusione (12,7/100). Il GTMI 2025 è 19,4/100. Il punteggio S2 è 2,7/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Antigua e Barbuda è valutata sufficiente ma disomogenea, con S3 pari a 5,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 71,8/100, sviluppo e diffusione dell'IA 12,7/100, penetrazione Internet 72,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Antigua e Barbuda ottiene S4 4,1/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Antigua e Barbuda, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto

sulla valutazione è misurato da S4=4,1/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Antigua e Barbuda è S5 3,2/10. La base ITU registra ITU GCI 18,2/100, Tier 5 - capacità iniziali; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (83/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Firmatario/invitato. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	1,5	Crimini finanziari	2,5
Reti criminali	3,5	Attori incorporati nello Stato	3,0
Attori stranieri	5,5	Attori del settore privato	2,5
Resilienza complessiva	4,7	Cooperazione internazionale	6,0
Politiche e norme nazionali	5,0	Forze dell'ordine	4,5
Antiriciclaggio	4,0	Prevenzione	5,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	3,4 - MODERATO

Rischio criminale connesso alle tecnologie. In Antigua e Barbuda il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 3,4/10, livello moderato. I reati che dipendono direttamente da sistemi informatici raggiungono 1,5/10; le frodi e i reati finanziari 2,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (5,5/10) e reti criminali (3,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Antigua e Barbuda assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Antigua e Barbuda, la resilienza complessiva è debole (4,7/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 5,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Antigua e Barbuda, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Antigua e Barbuda. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Antigua e Barbuda, In Antigua e Barbuda le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Antigua e Barbuda, Il livello governativo di Antigua e Barbuda presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Antigua e Barbuda, Sul piano militare e dual-use, Antigua e Barbuda mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Antigua e Barbuda, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Firmatario/invitato; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Antigua e Barbuda, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,6/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,8	2,7	5,2	4,1	3,2	4,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,9	5,6	5,9	6,1	5,2	5,6

Il GCRI di Antigua e Barbuda è 4,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,1/10), mentre il più basso è Supply chain (5,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Antigua e Barbuda, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Antigua e Barbuda, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Antigua e Barbuda, Dal punto di vista italiano, Antigua e Barbuda rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Antigua e Barbuda è indicata una cooperazione selettiva, coerente con il FOTR di 5,8/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Supply chain a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

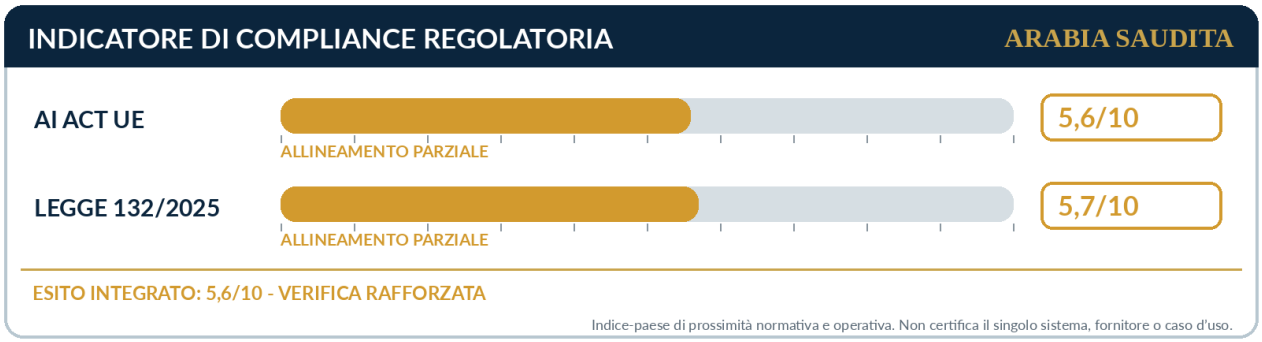
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Antigua e Barbuda: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Arabia Saudita

Posizione FOTR	**120**	**Area**	Asia	**Subregione**	Medio Oriente e Asia occidentale
Status	**Stato membro delle Nazioni Unite**	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	7/7 famiglie
FOTR / 10	**5,4**	**GCRI / 10**	**7,6**	**Classe operativa**	**Affidabilità selettiva**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Arabia Saudita, AI Act UE 5,6/10; legge 132/2025 5,7/10; esito integrato 5,6/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Arabia Saudita è stato membro delle nazioni unite collocato in Medio Oriente e Asia occidentale. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 9/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (7,6/10) è superiore al punteggio FOTR (5,4/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Arabia Saudita presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	100,0% / 44,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 483 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	96,0 / 99,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	100,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	74,8/100 - rank 15	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	25/100 - Non libero / Non libero (9/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,5 / 3,8 / 7,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Arabia Saudita, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Arabia Saudita le evidenze principali sono GTMI 99,6/100, EGDI 96,0/100, GCI 100,0/100, AI readiness 74,8/100. La dimensione più robusta è maturità infrastrutturale (9,4/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,9/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Arabia Saudita è 9,4/10. La base statistica rileva utenti Internet pari al 100,0% nel 2024; 44,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 483 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Arabia Saudita al posto 15 con un valore medio di 74,8/100; il pilastro migliore è governance (93,2/100), quello più debole è sviluppo e diffusione (54,5/100). Il GTMI 2025 è 99,6/100. Il punteggio S2 è 8,1/10 e indica una capacità elevata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Arabia Saudita è valutata sufficiente ma disomogenea, con S3 pari a 7,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 90,7/100, sviluppo e diffusione dell'IA 54,5/100, penetrazione Internet 100,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Arabia Saudita ottiene S4 5,9/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Arabia Saudita, Prevalenza statunitense ed europea nei sistemi strategici, con forte crescita di forniture cinesi e localizzazione industriale. L'impatto sulla valutazione è misurato da S4=5,9/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Arabia Saudita è S5 7,1/10. La base ITU registra ITU GCI 100,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure giuridiche (20,0/20). Freedom on the Net è 25/100 - Non libero, mentre Freedom in the World è Non libero (9/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Personal Data Protection Law, controlli NCA e regole di localizzazione/trasferimento; per dati strategici serve una verifica preventiva rafforzata.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,5	Crimini finanziari	8,5
Reti criminali	6,5	Attori incorporati nello Stato	9,0
Attori stranieri	3,5	Attori del settore privato	8,0
Resilienza complessiva	3,8	Cooperazione internazionale	5,0
Politiche e norme nazionali	4,0	Forze dell'ordine	3,5
Antiriciclaggio	5,0	Prevenzione	4,5
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	7,0 - ALTO

Rischio criminale connesso alle tecnologie. In Arabia Saudita il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 7,0/10, livello alto. I reati che dipendono direttamente da sistemi informatici raggiungono 7,5/10; le frodi e i reati finanziari 8,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e attori del settore privato (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Arabia Saudita assumono particolare rilevanza phishing e credential theft, ransomware, frodi d'investimento, attacchi a energia e servizi pubblici, abuso di cripto-attività e campagne che possono combinare profitto, spionaggio e pressione politica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Arabia Saudita, la resilienza complessiva è debole (3,8/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono deboli (4,0/10) e la capacità delle forze dell'ordine è debole (3,5/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 4,5/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Arabia Saudita, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Arabia Saudita. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Arabia Saudita, In Arabia Saudita le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Arabia Saudita, Il livello governativo di Arabia Saudita presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Arabia Saudita, Sul piano militare e dual-use, Arabia Saudita mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Arabia Saudita, Personal Data Protection Law, controlli NCA e regole di localizzazione/trasferimento; per dati strategici serve una verifica preventiva rafforzata. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Arabia Saudita, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,2/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,4	8,1	7,6	5,9	7,1	7,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,5	6,0	5,1	5,9	5,9	4,2

Il GCRI di Arabia Saudita è 7,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (6,0/10), mentre il più basso è Trasferibilità dati (4,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio	Medio-alto	Medio	Medio

La matrice applica il FOTR di 5,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Arabia Saudita, 3 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, IP e R&S. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Arabia Saudita, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Arabia Saudita, Dal punto di vista italiano, Arabia Saudita rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Arabia Saudita è indicata una cooperazione selettiva, coerente con il FOTR di 5,4/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

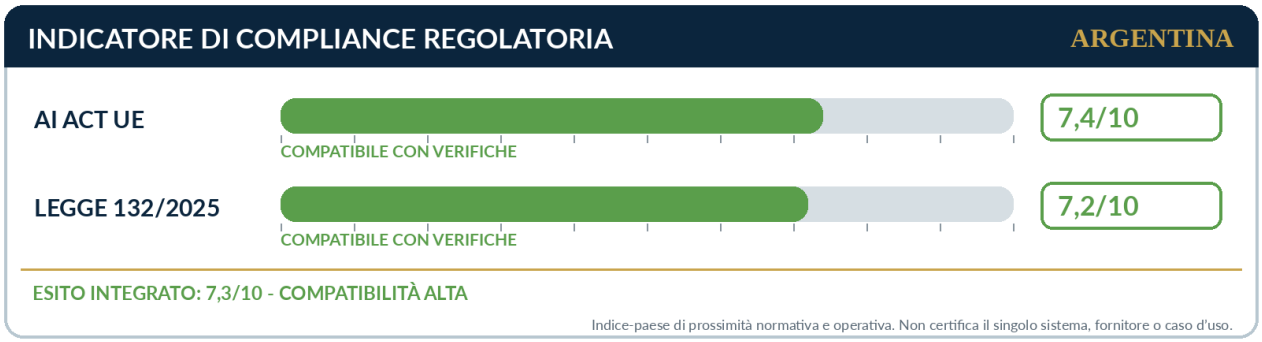
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Arabia Saudita: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Argentina

Posizione FOTR	47	Area	Americhe	Subregione	America meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	7,4	GCRI / 10	6,8	Classe operativa	Affidabilità favorevole ma condizionata

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Argentina, AI Act UE 7,4/10; legge 132/2025 7,2/10; esito integrato 7,3/10, classe «Compatibile con verifiche». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Prima dell'ingaggio occorre una analisi degli scostamenti mirata su trasparenza, governance dei dati, rappresentanza nell'UE, audit e rimedi contrattuali.

Premessa geopolitica e tecnologica

Nel quadro di Americhe, Argentina presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 85/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,8/10) e indice FOTR (7,4/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ambiente digitale di Argentina è complessivamente affidabile e aperto agli scambi. Per investimenti italiani è opportuno verificare la disciplina locale, la struttura dei fornitori e gli eventuali poteri pubblici di accesso.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	89,7% / 26,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	98,4% / 5.453 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	85,7 / 75,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	51,5/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	63,5/100 - rank 56	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	71/100 - Libero / Libero (85/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,0 / 5,7 / 5,3	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Argentina, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Argentina le evidenze principali sono GTMI 75,3/100, EGDI 85,7/100, GCI 51,5/100, AI readiness 63,5/100. La dimensione più robusta è maturità infrastrutturale (8,3/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,7/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Argentina è 8,3/10. La base statistica rileva utenti Internet pari al 89,7% nel 2024; 26,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 98,4% nel 2024; 5.453 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Argentina al posto 56 con un valore medio di 63,5/100; il pilastro migliore è governance (84,7/100), quello più debole è sviluppo e diffusione (32,1/100). Il GTMI 2025 è 75,3/100. Il punteggio S2 è 6,6/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Argentina è valutata sufficiente ma disomogenea, con S3 pari a 7,3/10. Le evidenze disponibili comprendono indice UN di capitale umano 93,3/100, sviluppo e diffusione dell'IA 32,1/100, penetrazione Internet 89,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Argentina ottiene S4 5,7/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Argentina, Prevalenza statunitense ed europea nei servizi, con presenza cinese nelle infrastrutture e capacità software locale. L'impatto sulla valutazione è misurato da S4=5,7/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Argentina è S5 6,0/10. La base ITU registra ITU GCI 51,5/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è sviluppo delle capacità (1,9/20). Freedom on the Net è 71/100 - Libero, mentre Freedom in the World è Libero (85/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Ley 25.326 sulla protezione dei dati, autorità di controllo e disciplina dei trasferimenti; decisione UE di adeguatezza, con necessità di verifica dell'effettività nel caso concreto.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,0	Crimini finanziari	4,5
Reti criminali	6,0	Attori incorporati nello Stato	6,0
Attori stranieri	5,5	Attori del settore privato	5,0
Resilienza complessiva	5,7	Cooperazione internazionale	6,0
Politiche e norme nazionali	6,5	Forze dell'ordine	5,5
Antiriciclaggio	6,0	Prevenzione	5,0
Supporto vittime e testimoni	5,5	Rischio operativo FOTR-CY	5,3 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Argentina restituisce un rischio FOTR-CY di 5,3/10 (significativo). La componente cyber-dipendente vale 6,0/10 e quella finanziaria 4,5/10; la risposta sistemica è valutata intermedia, con resilienza media di 5,7/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (6,0/10) e attori incorporati nello Stato (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Argentina assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Argentina, la resilienza complessiva è intermedia (5,7/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 5,0/10 e supporto a vittime e testimoni 5,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Argentina, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Argentina. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Argentina, In Argentina le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Argentina, Il livello governativo di Argentina presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Argentina, Sul piano militare e dual-use, Argentina mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Argentina, Ley 25.326 sulla protezione dei dati, autorità di controllo e disciplina dei trasferimenti; decisione UE di adeguatezza, con necessità di verifica dell'effettività nel caso concreto. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Argentina, È disponibile una decisione UE di adeguatezza. L'operatore italiano deve comunque controllare la portata della decisione, i trasferimenti successivi, le misure di sicurezza e le eventuali discipline settoriali. La componente FOTR di trasferibilità è 9,8/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,3	6,6	7,3	5,7	6,0	6,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
7,5	6,9	6,4	7,2	6,9	9,8

Il GCRI di Argentina è 6,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 7,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,8/10), mentre il più basso è Trasparenza istituzionale (6,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 7,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Argentina, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Argentina, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Argentina, Dal punto di vista italiano, Argentina rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Argentina è favorevole ma condizionata: il valore FOTR di 7,4/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Trasparenza istituzionale.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

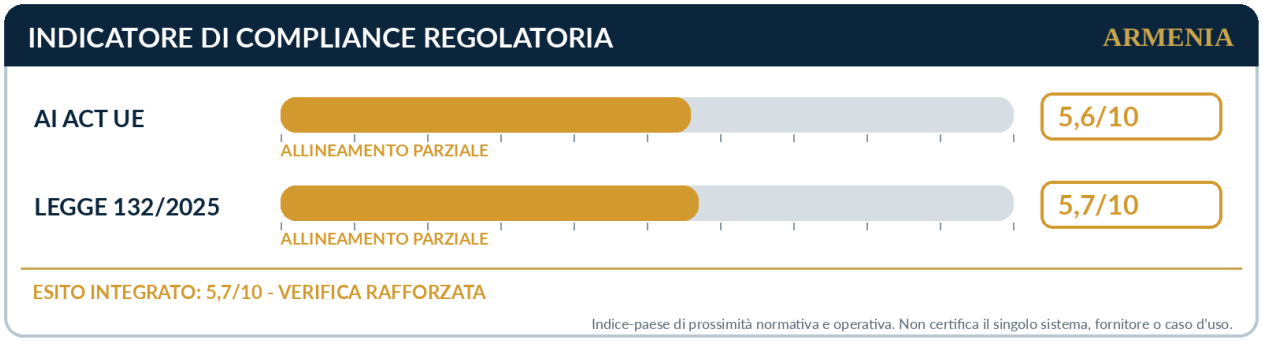
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Argentina: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Armenia

Posizione FOTR	92	Area	Asia	Subregione	Caucaso meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,7	GCRI / 10	6,1	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Armenia, AI Act UE 5,6/10; legge 132/2025 5,7/10; esito integrato 5,7/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Armenia, situato in Caucaso meridionale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 54/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,1/10) e indice FOTR (5,7/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il quadro di Armenia è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	81,3% / 20,3 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 1.735 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	84,2 / 76,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	53,8/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	39,0/100 - rank 103	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	72/100 - Libero / Parzialmente libero (54/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,5 / 5,6 / 3,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Armenia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Armenia le evidenze principali sono GTMI 76,9/100, EGDI 84,2/100, GCI 53,8/100, AI readiness 39,0/100. La dimensione più robusta è maturità infrastrutturale (7,8/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (5,2/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Armenia è 7,8/10. La base statistica rileva utenti Internet pari al 81,3% nel 2024; 20,3 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 1.735 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Armenia al posto 103 con un valore medio di 39,0/100; il pilastro migliore è adozione pubblica (57,4/100), quello più debole è sviluppo e diffusione (24,4/100). Il GTMI 2025 è 76,9/100. Il punteggio S2 è 5,2/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Armenia è valutata sufficiente ma disomogenea, con S3 pari a 6,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 85,6/100, sviluppo e diffusione dell'IA 24,4/100, penetrazione Internet 81,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Armenia ottiene S4 5,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Armenia, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo

societario e subfornitura. L'impatto sulla valutazione è misurato da S4=5,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Armenia è S5 6,0/10. La base ITU registra ITU GCI 53,8/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è organizzazione (2,8/20). Freedom on the Net è 72/100 - Libero, mentre Freedom in the World è Parzialmente libero (54/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge 2015 sulla protezione dei dati personali e quadro cyber in evoluzione; dipendenze infrastrutturali e geopolitiche da considerare.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,5	Crimini finanziari	3,5
Reti criminali	3,0	Attori incorporati nello Stato	3,5
Attori stranieri	3,0	Attori del settore privato	3,0
Resilienza complessiva	5,6	Cooperazione internazionale	7,0
Politiche e norme nazionali	6,5	Forze dell'ordine	6,5
Antiriciclaggio	5,5	Prevenzione	4,5
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	3,6 - MODERATO

Pressione del crimine digitale. Il profilo di Armenia restituisce un rischio FOTR-CY di 3,6/10 (moderato). La componente cyber-dipendente vale 3,5/10 e quella finanziaria 3,5/10; la risposta sistemica è valutata intermedia, con resilienza media di 5,6/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (3,5/10) e reti criminali (3,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Armenia assumono particolare rilevanza ransomware come servizio, malware sottrattori di informazioni, infrastrutture di hosting permissive, DDoS, furto di credenziali, estorsione dei dati e possibili sovrapposizioni tra criminalità professionale e finalità geopolitiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Armenia, la resilienza complessiva è intermedia (5,6/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è intermedia (6,5/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 4,5/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Armenia, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; blocco di hosting e ASN ad alta reputazione negativa, ricerca proattiva delle minacce su malware sottrattori di informazioni e controllo dei canali RDP/VPN; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Armenia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Armenia, In Armenia le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Armenia, Il livello governativo di Armenia presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Armenia, Sul piano militare e dual-use, Armenia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Armenia, Legge 2015 sulla protezione dei dati personali e quadro cyber in evoluzione; dipendenze infrastrutturali e geopolitiche da considerare. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Armenia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,3/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,8	5,2	6,2	5,3	6,0	6,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,7	6,6	5,2	5,8	5,6	5,3

Il GCRI di Armenia è 6,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Maturità cyber (6,6/10), mentre il più basso è Trasparenza istituzionale (5,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Armenia, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Armenia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Armenia, Dal punto di vista italiano, Armenia rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Armenia è indicata una cooperazione selettiva, coerente con il FOTR di 5,7/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasparenza istituzionale a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

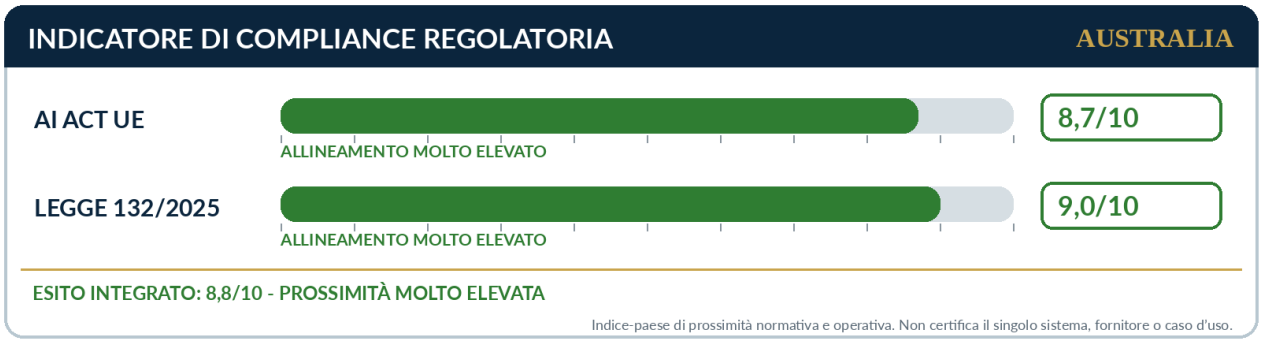
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Armenia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Australia

Posizione FOTR	14	**Area**	Oceania	**Subregione**	Australia e Nuova Zelanda
Status	Stato membro delle Nazioni Unite	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	7/7 famiglie
FOTR / 10	8,9	**GCRI / 10**	8,7	**Classe operativa**	**Affidabilità alta**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Australia, AI Act UE 8,7/10; legge 132/2025 9,0/10; esito integrato 8,8/10, classe «Allineamento molto elevato». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Per un operatore italiano, Australia non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La partecipazione all'ecosistema Five Eyes rafforza l'integrazione informativa e tecnologica con il blocco anglosassone, ma rende necessario valutare i poteri di accesso extraterritoriale e la concentrazione cloud. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 94/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,7/10) e indice FOTR (8,9/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per un operatore italiano, Australia costituisce un ambiente digitale ad alta affidabilità: connettività, supervisione e continuità sono solide. La valutazione non deve però trascurare subfornitori, accessi transfrontalieri e tecnologie dual-use.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	96,1% / 36,5 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 44.299 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	95,8 / 98,5	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	96,2/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	79,6/100 - rank 9	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	75/100 - Libero / Libero (94/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	8,0 / 7,5 / 5,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Australia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Australia le evidenze principali sono GTMI 98,5/100, EGDI 95,8/100, GCI 96,2/100, AI readiness 79,6/100. La dimensione più robusta è maturità infrastrutturale (9,5/10), mentre la criticità relativa riguarda indipendenza della supply chain (8,0/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Australia è 9,5/10. La base statistica rileva utenti Internet pari al 96,1% nel 2024; 36,5 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 44.299 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Australia al posto 9 con un valore medio di 79,6/100; il pilastro migliore è politiche pubbliche (100,0/100), quello più debole è sviluppo e diffusione (62,7/100). Il GTMI 2025 è 98,5/100. Il punteggio S2 è 8,4/10 e indica una capacità elevata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Australia è valutata solida, con S3 pari a 8,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 100,0/100, sviluppo e diffusione dell'IA 62,7/100, penetrazione Internet 96,1%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Australia ottiene S4 8,0/10 e presenta buona capacità di diversificazione. La provenienza prevalente stimata è Stati Uniti; l'indicatore di indipendenza disponibile è 7,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Australia, Fornitura domestica e statunitense, con integrazione Five Eyes e componentistica asiatica. L'impatto sulla valutazione è misurato da S4=8,0/10 e dal proxy di indipendenza 7,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Australia è S5 9,1/10. La base ITU registra ITU GCI 96,2/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure tecniche (17,9/20). Freedom on the Net è 75/100 - Libero, mentre Freedom in the World è Libero (94/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Privacy Act 1988, Notifiable Data Breaches, Security of Critical Infrastructure Act e normativa cyber federale; riforme privacy e sicurezza in progressivo rafforzamento.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	8,0	Crimini finanziari	7,0
Reti criminali	5,0	Attori incorporati nello Stato	2,0
Attori stranieri	4,0	Attori del settore privato	3,0
Resilienza complessiva	7,5	Cooperazione internazionale	9,0
Politiche e norme nazionali	8,0	Forze dell'ordine	8,0
Antiriciclaggio	7,0	Prevenzione	7,0
Supporto vittime e testimoni	6,5	Rischio operativo FOTR-CY	5,2 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Australia presenta un'esposizione stimata significativa (5,2/10): reati cyber-dipendenti 8,0/10, crimini finanziari 7,0/10 e resilienza 7,5/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (5,0/10) e attori stranieri (4,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Australia assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Australia, la resilienza complessiva è robusta (7,5/10); la cooperazione internazionale è robusta (9,0/10), le politiche e norme nazionali sono robuste (8,0/10) e la capacità delle forze dell'ordine è robusta (8,0/10). Completano il quadro antiriciclaggio 7,0/10, prevenzione 7,0/10 e supporto a vittime e testimoni 6,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Australia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Australia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Australia, In Australia le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La

superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Australia, Il livello governativo di Australia presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Australia, Sul piano militare e dual-use, Australia mostra stretta cooperazione con ecosistemi occidentali e capacità dual-use significative. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Australia, Privacy Act 1988, Notifiable Data Breaches, Security of Critical Infrastructure Act e normativa cyber federale; riforme privacy e sicurezza in progressivo rafforzamento. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Australia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 7,6/10 e il rischio sui dati personali è Medio-basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,5	8,4	8,5	8,0	9,1	8,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,6	10,0	8,1	10,0	9,0	7,6

Il GCRI di Australia è 8,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,9/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Maturità cyber (10,0/10), mentre il più basso è Trasferibilità dati (7,6/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-basso	Basso	Basso	Basso	Basso	Basso

La matrice applica il FOTR di 8,9/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Australia, la cautela si concentra su 1 ambiti a rischio intermedio: Dati personali. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Australia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Australia, Dal punto di vista italiano, Australia rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Australia, il FOTR di 8,9/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasferibilità dati (7,6/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

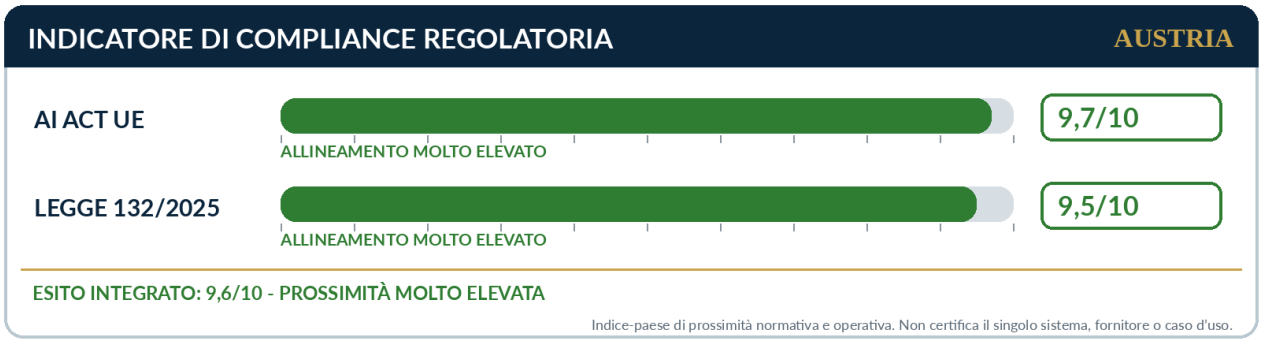
Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Australia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Austria

Posizione FOTR	**15**	**Area**	Europa	**Subregione**	Europa occidentale e centrale
Status	**Stato membro delle Nazioni Unite**	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	**8,9**	**GCRI / 10**	**8,0**	**Classe operativa**	**Affidabilità alta**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Austria, AI Act UE 9,7/10; legge 132/2025 9,5/10; esito integrato 9,6/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Austria è stato membro delle nazioni unite collocato in Europa occidentale e centrale. L'appartenenza all'Unione europea inserisce il Paese nel mercato digitale unico, nel sistema GDPR e nelle principali discipline comuni su cybersicurezza, dati e intelligenza artificiale. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 94/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,0/10) e indice FOTR (8,9/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per un operatore italiano, Austria costituisce un ambiente digitale ad alta affidabilità: connettività, supervisione e continuità sono solide. La valutazione non deve però trascurare subfornitori, accessi transfrontalieri e tecnologie dual-use.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	91,9% / 30,1 per 100	2025/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 47.132 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	90,7 / 92,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	89,2/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	72,3/100 - rank 20	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (94/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 7,5 / 4,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Austria, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Austria le evidenze principali sono GTMI 92,9/100, EGDI 90,7/100, GCI 89,2/100, AI readiness 72,3/100. La dimensione più robusta è maturità infrastrutturale (9,2/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,3/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Austria è 9,2/10. La base statistica rileva utenti Internet pari al 91,9% nel 2025; 30,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 47.132 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Austria al posto 20 con un valore medio di 72,3/100; il pilastro migliore è governance (87,0/100), quello più debole è sviluppo e diffusione (58,1/100). Il GTMI 2025 è 92,9/100. Il punteggio S2 è 7,7/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Austria è valutata solida, con S3 pari a 8,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 90,0/100, sviluppo e diffusione dell'IA 58,1/100, penetrazione Internet 91,9%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Austria ottiene S4 6,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Austria, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Austria è S5 8,7/10. La base ITU registra ITU GCI 89,2/100, Tier 2 - avanzato; il pilastro relativamente più debole è cooperazione (16,6/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (94/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, Datenschutzgesetz e disciplina nazionale di attuazione NIS2; quadro UE direttamente applicabile su AI, dati, piattaforme e prodotti digitali.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	6,0
Reti criminali	4,0	Attori incorporati nello Stato	4,0
Attori stranieri	6,5	Attori del settore privato	5,0
Resilienza complessiva	7,5	Cooperazione internazionale	7,5
Politiche e norme nazionali	8,0	Forze dell'ordine	9,0
Antiriciclaggio	6,5	Prevenzione	7,5
Supporto vittime e testimoni	8,0	Rischio operativo FOTR-CY	4,6 - MODERATO

Pressione del crimine digitale. Il profilo di Austria restituisce un rischio FOTR-CY di 4,6/10 (moderato). La componente cyber-dipendente vale 5,5/10 e quella finanziaria 6,0/10; la risposta sistemica è valutata robusta, con resilienza media di 7,5/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (6,5/10) e attori del settore privato (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Austria assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Austria, la resilienza complessiva è robusta (7,5/10); la cooperazione internazionale è robusta (7,5/10), le politiche e norme nazionali sono robuste (8,0/10) e la capacità delle forze dell'ordine è robusta (9,0/10). Completano il quadro antiriciclaggio 6,5/10, prevenzione 7,5/10 e supporto a vittime e testimoni 8,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Austria, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Austria. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Austria, In Austria le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Austria, Il livello governativo di Austria presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Austria, Sul piano militare e dual-use, Austria mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Austria, GDPR, Datenschutzgesetz e disciplina nazionale di attuazione NIS2; quadro UE direttamente applicabile su AI, dati, piattaforme e prodotti digitali. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Austria, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,8/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,2	7,7	8,1	6,3	8,7	8,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,3	8,2	8,5	9,5	7,6	9,8

Il GCRI di Austria è 8,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,9/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,8/10), mentre il più basso è Supply chain (7,6/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Medio-basso	Basso	Basso	Basso

La matrice applica il FOTR di 8,9/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Austria, la cautela si concentra su 1 ambiti a rischio intermedio: Cloud e infrastrutture. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Austria, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Austria, Dal punto di vista italiano, Austria rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Austria, il FOTR di 8,9/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (7,6/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

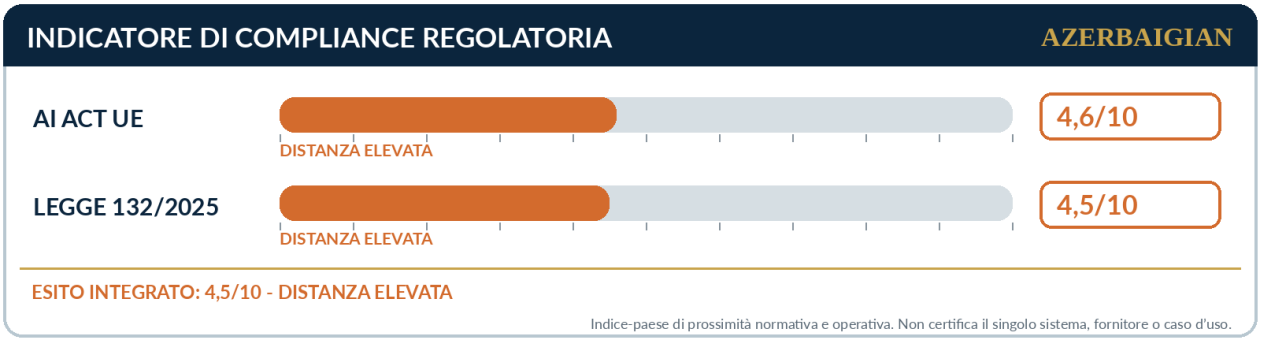
Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Austria: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Azerbaigian

Posizione FOTR	161	Area	Asia	Subregione	Caucaso meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	4,4	GCRI / 10	6,3	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Azerbaigian, AI Act UE 4,6/10; legge 132/2025 4,5/10; esito integrato 4,5/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Nel quadro di Asia, Azerbaigian presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 6/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (6,3/10) è superiore al punteggio FOTR (4,4/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Azerbaigian presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	90,8% / 21,8 per 100	2025/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 541 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	76,1 / 76,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	93,8/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	54,1/100 - rank 69	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	34/100 - Non libero / Non libero (6/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 4,0 / 5,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Azerbaigian, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Azerbaigian le evidenze principali sono GTMI 76,9/100, EGDI 76,1/100, GCI 93,8/100, AI readiness 54,1/100. La dimensione più robusta è maturità infrastrutturale (7,8/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,1/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Azerbaigian è 7,8/10. La base statistica rileva utenti Internet pari al 90,8% nel 2025; 21,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 541 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Azerbaigian al posto 69 con un valore medio di 54,1/100; il pilastro migliore è adozione pubblica (67,0/100), quello più debole è sviluppo e diffusione (36,1/100). Il GTMI 2025 è 76,9/100. Il punteggio S2 è 6,1/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Azerbaigian è valutata sufficiente ma disomogenea, con S3 pari a 5,7/10. Le evidenze disponibili comprendono indice UN di capitale umano 72,3/100, sviluppo e diffusione dell'IA 36,1/100, penetrazione Internet 90,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Azerbaigian ottiene S4 5,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Azerbaigian, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo

societario e subfornitura. L'impatto sulla valutazione è misurato da S4=5,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Azerbaigian è S5 6,7/10. La base ITU registra ITU GCI 93,8/100, Tier 2 - avanzato; il pilastro relativamente più debole è sviluppo delle capacità (17,7/20). Freedom on the Net è 34/100 - Non libero, mentre Freedom in the World è Non libero (6/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge sui dati personali e disciplina delle telecomunicazioni; elevato ruolo statale e limitata trasparenza degli accessi pubblici.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	5,5
Reti criminali	5,5	Attori incorporati nello Stato	8,5
Attori stranieri	6,0	Attori del settore privato	4,0
Resilienza complessiva	4,0	Cooperazione internazionale	5,0
Politiche e norme nazionali	4,0	Forze dell'ordine	4,5
Antiriciclaggio	4,0	Prevenzione	4,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	5,2 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Azerbaigian il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,2/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 3,0/10; le frodi e i reati finanziari 5,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,5/10) e attori stranieri (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Azerbaigian assumono particolare rilevanza ransomware come servizio, malware sottrattori di informazioni, infrastrutture di hosting permissive, DDoS, furto di credenziali, estorsione dei dati e possibili sovrapposizioni tra criminalità professionale e finalità geopolitiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Azerbaigian, la resilienza complessiva è debole (4,0/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono deboli (4,0/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Azerbaigian, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; blocco di hosting e ASN ad alta reputazione negativa, ricerca proattiva delle minacce su malware sottrattori di informazioni e controllo dei canali RDP/VPN; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Azerbaigian. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Azerbaigian, In Azerbaigian le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La

disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Azerbaigian, Il livello governativo di Azerbaigian presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Azerbaigian, Sul piano militare e dual-use, Azerbaigian mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Azerbaigian, Legge sui dati personali e disciplina delle telecomunicazioni; elevato ruolo statale e limitata trasparenza degli accessi pubblici. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Azerbaigian, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,2/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,8	6,1	5,7	5,1	6,7	6,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,5	4,7	4,3	4,2	4,2	4,2

Il GCRI di Azerbaigian è 6,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (4,7/10), mentre il più basso è Compatibilità strategica (4,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Azerbaigian, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Azerbaigian, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Azerbaigian, Dal punto di vista italiano, Azerbaigian rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Azerbaigian ricade nella fascia di alto rischio (4,4/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

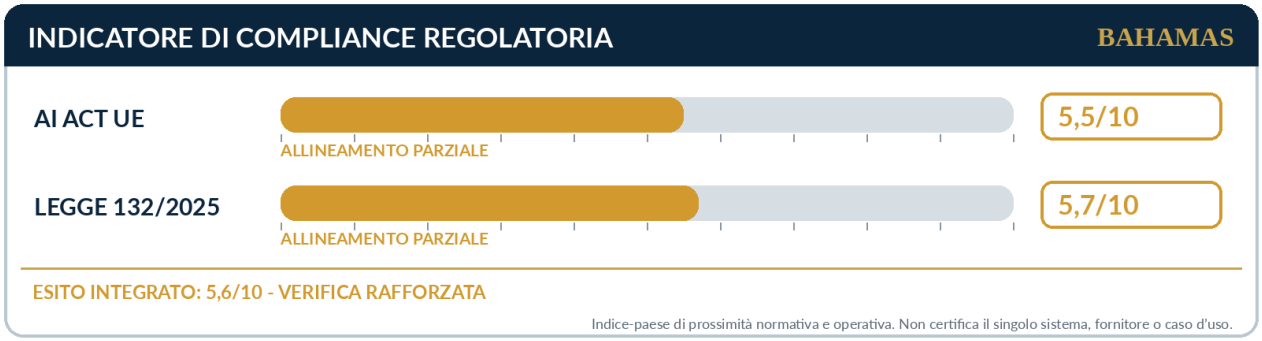
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Azerbaigian: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Bahamas

Posizione FOTR	93	Area	Americhe	Subregione	Caraibi
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,7	GCRI / 10	5,3	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Bahamas, AI Act UE 5,5/10; legge 132/2025 5,7/10; esito integrato 5,6/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Bahamas, situato in Caraibi, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 90/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,3/10) e indice FOTR (5,7/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Bahamas dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	92,5% / 25,3 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 6.355 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	71,4 / 50,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	34,0/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	30,3/100 - rank 123	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (90/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 5,6 / 3,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Bahamas, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Bahamas le evidenze principali sono GTMI 50,2/100, EGDI 71,4/100, GCI 34,0/100, AI readiness 30,3/100. La dimensione più robusta è maturità infrastrutturale (8,4/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,8/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Bahamas è 8,4/10. La base statistica rileva utenti Internet pari al 92,5% nel 2024; 25,3 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 6.355 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Bahamas al posto 123 con un valore medio di 30,3/100; il pilastro migliore è governance (53,6/100), quello più debole è politiche pubbliche (8,0/100). Il GTMI 2025 è 50,2/100. Il punteggio S2 è 3,8/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Bahamas è valutata sufficiente ma disomogenea, con S3 pari a 5,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 73,8/100, sviluppo e diffusione dell'IA 14,6/100, penetrazione Internet 92,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Bahamas ottiene S4 4,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Bahamas, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=4,6/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Bahamas è S5 4,2/10. La base ITU registra ITU GCI 34,0/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (3,2/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (90/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	4,0
Reti criminali	3,0	Attori incorporati nello Stato	3,0
Attori stranieri	6,5	Attori del settore privato	3,5
Resilienza complessiva	5,6	Cooperazione internazionale	6,5
Politiche e norme nazionali	7,0	Forze dell'ordine	6,5
Antiriciclaggio	5,5	Prevenzione	6,0
Supporto vittime e testimoni	7,0	Rischio operativo FOTR-CY	3,9 - MODERATO

Sintesi del rischio cybercrime. Bahamas presenta un'esposizione stimata moderata (3,9/10): reati cyber-dipendenti 3,0/10, crimini finanziari 4,0/10 e resilienza 5,6/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (6,5/10) e attori del settore privato (3,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Bahamas assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Bahamas, la resilienza complessiva è intermedia (5,6/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è intermedia (6,5/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 7,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Bahamas, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Bahamas. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Bahamas, In Bahamas le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Bahamas, Il livello governativo di Bahamas presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Bahamas, Sul piano militare e dual-use, Bahamas mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Bahamas, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Bahamas, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,5/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,4	3,8	5,4	4,6	4,2	5,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,1	5,4	5,7	5,9	5,4	5,5

Il GCRI di Bahamas è 5,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (6,1/10), mentre il più basso è Maturità cyber (5,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Bahamas, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Bahamas, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Bahamas, Dal punto di vista italiano, Bahamas rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Bahamas è indicata una cooperazione selettiva, coerente con il FOTR di 5,7/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Maturità cyber a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

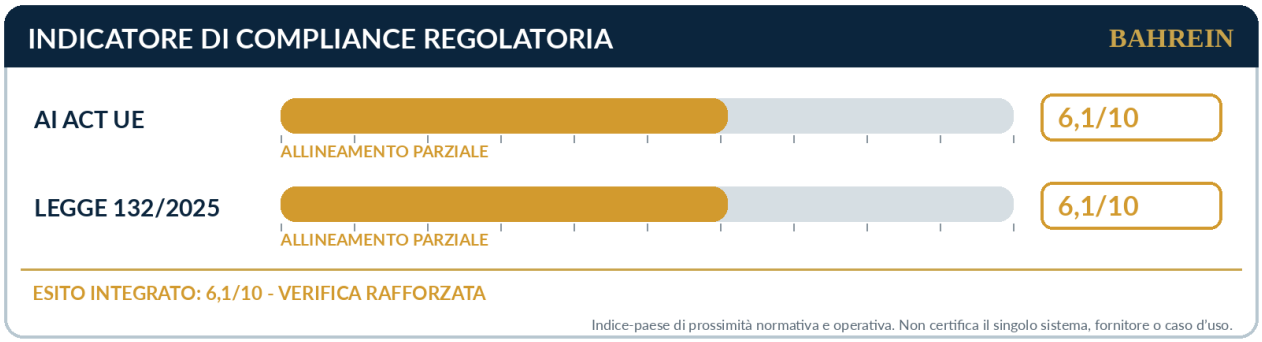
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Bahamas: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Bahrein

Posizione FOTR	73	**Area**	Asia	**Subregione**	Medio Oriente e Asia occidentale
Status	Stato membro delle Nazioni Unite	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	7/7 famiglie
FOTR / 10	6,0	**GCRI / 10**	7,2	**Classe operativa**	**Affidabilità selettiva**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Bahrein, AI Act UE 6,1/10; legge 132/2025 6,1/10; esito integrato 6,1/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Bahrein non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 12/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (7,2/10) è superiore al punteggio FOTR (6,0/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Bahrein dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	100,0% / 17,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 7.064 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	92,0 / 93,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	97,9/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	59,7/100 - rank 48	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	30/100 - Non libero / Non libero (12/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,0 / 5,3 / 5,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Bahrein, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Bahrein le evidenze principali sono GTMI 93,6/100, EGDI 92,0/100, GCI 97,9/100, AI readiness 59,7/100. La dimensione più robusta è maturità infrastrutturale (8,6/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,8/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Bahrein è 8,6/10. La base statistica rileva utenti Internet pari al 100,0% nel 2024; 17,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 7.064 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Bahrein al posto 48 con un valore medio di 59,7/100; il pilastro migliore è adozione pubblica (83,4/100), quello più debole è politiche pubbliche (46,5/100). Il GTMI 2025 è 93,6/100. Il punteggio S2 è 7,0/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Bahrein è valutata sufficiente ma disomogenea, con S3 pari a 7,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 86,8/100, sviluppo e diffusione dell'IA 48,5/100, penetrazione Internet 100,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Bahrein ottiene S4 5,8/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Bahrein, Forte integrazione con fornitori statunitensi e britannici; mercato commerciale multi-origine. L'impatto sulla valutazione è misurato da S4=5,8/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Bahrein è S5 7,3/10. La base ITU registra ITU GCI 97,9/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è cooperazione (17,9/20). Freedom on the Net è 30/100 - Non libero, mentre Freedom in the World è Non libero (12/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Personal Data Protection Law 2018 e disciplina cyber; trasferimenti UE mediante garanzie e verifica dell'indipendenza dei rimedi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,0	Crimini finanziari	7,0
Reti criminali	6,0	Attori incorporati nello Stato	4,5
Attori stranieri	5,0	Attori del settore privato	6,0
Resilienza complessiva	5,3	Cooperazione internazionale	7,0
Politiche e norme nazionali	5,5	Forze dell'ordine	4,5
Antiriciclaggio	5,5	Prevenzione	5,5
Supporto vittime e testimoni	6,0	Rischio operativo FOTR-CY	5,9 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Bahrein restituisce un rischio FOTR-CY di 5,9/10 (significativo). La componente cyber-dipendente vale 7,0/10 e quella finanziaria 7,0/10; la risposta sistemica è valutata debole, con resilienza media di 5,3/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (6,0/10) e attori del settore privato (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Bahrein assumono particolare rilevanza phishing e credential theft, ransomware, frodi d'investimento, attacchi a energia e servizi pubblici, abuso di cripto-attività e campagne che possono combinare profitto, spionaggio e pressione politica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Bahrein, la resilienza complessiva è debole (5,3/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 5,5/10 e supporto a vittime e testimoni 6,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Bahrein, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Bahrein. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Bahrein, In Bahrein le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Bahrein, Il livello governativo di Bahrein presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Bahrein, Sul piano militare e dual-use, Bahrein mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Bahrein, Personal Data Protection Law 2018 e disciplina cyber; trasferimenti UE mediante garanzie e verifica dell'indipendenza dei rimedi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Bahrein, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,6/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,6	7,0	7,1	5,8	7,3	7,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,1	6,6	5,5	6,1	6,0	5,6

Il GCRI di Bahrein è 7,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (6,6/10), mentre il più basso è Trasparenza istituzionale (5,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Bahrein, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Bahrein, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Bahrein, Dal punto di vista italiano, Bahrein rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Bahrein è indicata una cooperazione selettiva, coerente con il FOTR di 6,0/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasparenza istituzionale a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

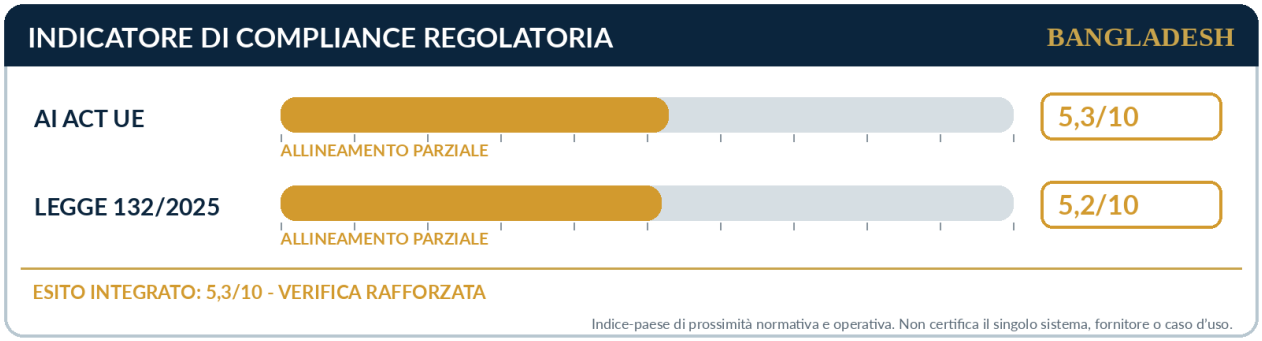
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Bahrein: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Bangladesh

Posizione FOTR	124	Area	Asia	Subregione	Asia meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,2	GCRI / 10	5,9	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Bangladesh, AI Act UE 5,3/10; legge 132/2025 5,2/10; esito integrato 5,3/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Bangladesh è stato membro delle nazioni unite collocato in Asia meridionale. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 44/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,9/10) e indice FOTR (5,2/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Bangladesh presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	53,4% / 8,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	99,5% / 527 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	65,7 / 88,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	97,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	51,9/100 - rank 75	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	45/100 - Parzialmente libero / Parzialmente libero (44/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 4,1 / 5,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Bangladesh, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Bangladesh le evidenze principali sono GTMI 88,2/100, EGDI 65,7/100, GCI 97,0/100, AI readiness 51,9/100. La dimensione più robusta è postura di sicurezza cyber (7,3/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (5,0/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Bangladesh è 5,7/10. La base statistica rileva utenti Internet pari al 53,4% nel 2024; 8,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 99,5% nel 2024; 527 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Bangladesh al posto 75 con un valore medio di 51,9/100; il pilastro migliore è adozione pubblica (82,8/100), quello più debole è sviluppo e diffusione (27,0/100). Il GTMI 2025 è 88,2/100. Il punteggio S2 è 6,0/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Bangladesh è valutata sufficiente ma disomogenea, con S3 pari a 5,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 58,3/100, sviluppo e diffusione dell'IA 27,0/100, penetrazione Internet 53,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Bangladesh ottiene S4 5,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Bangladesh, Forte presenza cinese e asiatica nelle reti e nell'hardware; servizi software locali e internazionali. L'impatto sulla valutazione è misurato da S4=5,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Bangladesh è S5 7,3/10. La base ITU registra ITU GCI 97,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure giuridiche (17,4/20). Freedom on the Net è 45/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (44/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	5,0
Reti criminali	6,0	Attori incorporati nello Stato	7,0
Attori stranieri	4,0	Attori del settore privato	4,0
Resilienza complessiva	4,1	Cooperazione internazionale	5,5
Politiche e norme nazionali	5,0	Forze dell'ordine	4,0
Antiriciclaggio	4,5	Prevenzione	3,0
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	5,4 - SIGNIFICATIVO

Quadro criminale digitale. Per Bangladesh, l'indice operativo FOTR-CY è 5,4/10, classe significativa. Il mercato dei reati cyber-dipendenti è intermedio (5,0/10), mentre i crimini finanziari sono intermedi (5,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,0/10) e reti criminali (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Bangladesh assumono particolare rilevanza compromissione delle caselle di posta aziendale, frodi da call center, abuso di portafogli digitali mobili, identità sintetiche, ransomware, phishing bancario e triangolazioni transfrontaliere dei proventi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Bangladesh, la resilienza complessiva è debole (4,1/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 3,0/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Bangladesh, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Bangladesh. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Bangladesh, In Bangladesh le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Bangladesh, Il livello governativo di Bangladesh presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Bangladesh, Sul piano militare e dual-use, Bangladesh mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Bangladesh, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Bangladesh, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,0/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
5,7	6,0	5,0	5,3	7,3	5,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,4	5,7	4,8	5,0	5,2	5,0

Il GCRI di Bangladesh è 5,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (5,7/10), mentre il più basso è Trasparenza istituzionale (4,8/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 5,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Bangladesh, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Bangladesh, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Bangladesh, Dal punto di vista italiano, Bangladesh rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Bangladesh è indicata una cooperazione selettiva, coerente con il FOTR di 5,2/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

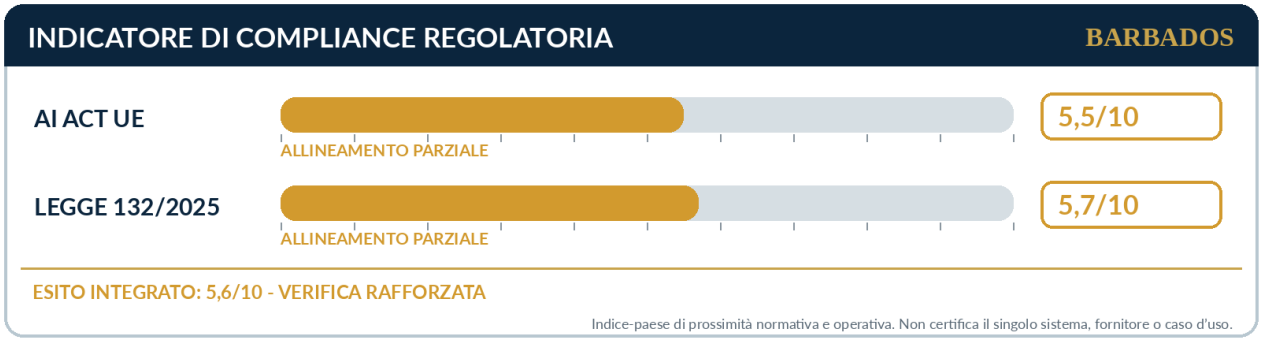
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Bangladesh: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Barbados

Posizione FOTR	81	Area	Americhe	Subregione	Caraibi
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,8	GCRI / 10	5,0	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Barbados, AI Act UE 5,5/10; legge 132/2025 5,7/10; esito integrato 5,6/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Americhe, Barbados presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 94/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,0/10) e indice FOTR (5,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Barbados dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	70,4% / 37,5 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 1.172 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	68,2 / 31,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	36,5/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	22,8/100 - rank 155	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (94/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,5 / 6,1 / 3,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Barbados, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Barbados le evidenze principali sono GTMI 31,8/100, EGDI 68,2/100, GCI 36,5/100, AI readiness 22,8/100. La dimensione più robusta è maturità infrastrutturale (7,9/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Barbados è 7,9/10. La base statistica rileva utenti Internet pari al 70,4% nel 2024; 37,5 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 100,0% nel 2024; 1.172 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Barbados al posto 155 con un valore medio di 22,8/100; il pilastro migliore è governance (40,8/100), quello più debole è adozione pubblica (6,2/100). Il GTMI 2025 è 31,8/100. Il punteggio S2 è 2,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Barbados è valutata sufficiente ma disomogenea, con S3 pari a 5,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 78,5/100, sviluppo e diffusione dell'IA 14,0/100, penetrazione Internet 70,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Barbados ottiene S4 4,3/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Barbados, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=4,3/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Barbados è S5 4,4/10. La base ITU registra ITU GCI 36,5/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (3,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (94/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,5	Crimini finanziari	2,5
Reti criminali	4,0	Attori incorporati nello Stato	3,0
Attori stranieri	3,0	Attori del settore privato	1,5
Resilienza complessiva	6,1	Cooperazione internazionale	7,5
Politiche e norme nazionali	7,0	Forze dell'ordine	7,0
Antiriciclaggio	5,5	Prevenzione	6,0
Supporto vittime e testimoni	5,5	Rischio operativo FOTR-CY	3,1 - MODERATO

Quadro criminale digitale. Per Barbados, l'indice operativo FOTR-CY è 3,1/10, classe moderata. Il mercato dei reati cyber-dipendenti è limitato o poco osservabile (2,5/10), mentre i crimini finanziari sono limitati o poco osservabili (2,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (4,0/10) e attori incorporati nello Stato (3,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Barbados assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Barbados, la resilienza complessiva è intermedia (6,1/10); la cooperazione internazionale è robusta (7,5/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è intermedia (7,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 5,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Barbados, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Barbados. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Barbados, In Barbados le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Barbados, Il livello governativo di Barbados presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Barbados, Sul piano militare e dual-use, Barbados mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Barbados, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Barbados, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,7/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,9	2,9	5,5	4,3	4,4	5,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,8	5,5	6,1	6,1	5,3	5,7

Il GCRI di Barbados è 5,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasparenza istituzionale (6,1/10), mentre il più basso è Supply chain (5,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Barbados, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Barbados, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Barbados, Dal punto di vista italiano, Barbados rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Barbados è indicata una cooperazione selettiva, coerente con il FOTR di 5,8/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Supply chain a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

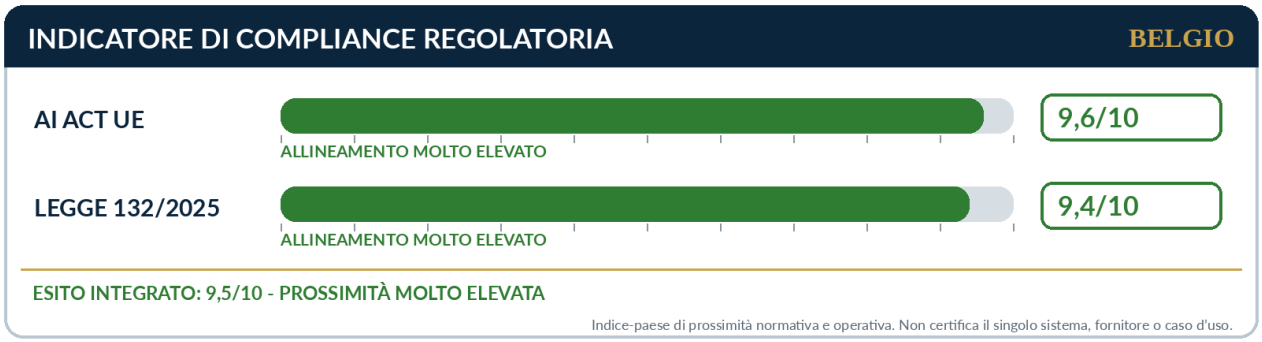
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Barbados: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Belgio

Posizione FOTR	18	Area	Europa	Subregione	Europa occidentale e centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,8	GCRI / 10	7,9	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Belgio, AI Act UE 9,6/10; legge 132/2025 9,4/10; esito integrato 9,5/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Belgio, situato in Europa occidentale e centrale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 95/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,9/10) e indice FOTR (8,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il sistema digitale di Belgio è avanzato e integrato con standard internazionali. Le principali criticità non sono di base istituzionale, ma riguardano supply chain, concentrazione dei servizi e gestione delle eccezioni di sicurezza nazionale.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	95,8% / 44,2 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 36.732 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	81,2 / 83,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	96,8/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	68,8/100 - rank 30	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (95/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,5 / 7,2 / 5,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Belgio, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Belgio le evidenze principali sono GTMI 83,0/100, EGDI 81,2/100, GCI 96,8/100, AI readiness 68,8/100. La dimensione più robusta è maturità infrastrutturale (9,4/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,2/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Belgio è 9,4/10. La base statistica rileva utenti Internet pari al 95,8% nel 2024; 44,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 36.732 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Belgio al posto 30 con un valore medio di 68,8/100; il pilastro migliore è politiche pubbliche (85,0/100), quello più debole è sviluppo e diffusione (49,8/100). Il GTMI 2025 è 83,0/100. Il punteggio S2 è 7,1/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Belgio è valutata sufficiente ma disomogenea, con S3 pari a 7,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 84,4/100, sviluppo e diffusione dell'IA 49,8/100, penetrazione Internet 95,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Belgio ottiene S4 6,2/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open

source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Belgio, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario, luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,2/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Belgio è S5 9,2/10. La base ITU registra ITU GCI 96,8/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure tecniche (18,1/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (95/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, Data Protection Act belga e normativa di sicurezza delle reti; applicazione del corpus digitale e cyber dell'Unione europea.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,5	Crimini finanziari	6,5
Reti criminali	5,5	Attori incorporati nello Stato	2,5
Attori stranieri	6,0	Attori del settore privato	3,5
Resilienza complessiva	7,2	Cooperazione internazionale	8,5
Politiche e norme nazionali	7,5	Forze dell'ordine	6,5
Antiriciclaggio	7,0	Prevenzione	7,5
Supporto vittime e testimoni	8,0	Rischio operativo FOTR-CY	5,0 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Belgio il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,0/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 6,5/10; le frodi e i reati finanziari 6,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (6,0/10) e reti criminali (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Belgio assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Belgio, la resilienza complessiva è intermedia (7,2/10); la cooperazione internazionale è robusta (8,5/10), le politiche e norme nazionali sono robuste (7,5/10) e la capacità delle forze dell'ordine è intermedia (6,5/10). Completano il quadro antiriciclaggio 7,0/10, prevenzione 7,5/10 e supporto a vittime e testimoni 8,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Belgio, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Belgio. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Belgio, In Belgio le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Belgio, Il livello governativo di Belgio presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Belgio, Sul piano militare e dual-use, Belgio mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Belgio, GDPR, Data Protection Act belga e normativa di sicurezza delle reti; applicazione del corpus digitale e cyber dell'Unione europea. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Belgio, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,8/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,4	7,1	7,6	6,2	9,2	7,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,2	8,1	8,5	9,3	7,7	9,8

Il GCRI di Belgio è 7,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,8/10), mentre il più basso è Supply chain (7,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Medio-basso	Basso	Medio-basso	Basso

La matrice applica il FOTR di 8,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Belgio, la cautela si concentra su 2 ambiti a rischio intermedio: Cloud e infrastrutture, Pubblica amministrazione. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Belgio, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Belgio, Dal punto di vista italiano, Belgio rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Belgio, il FOTR di 8,8/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (7,7/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

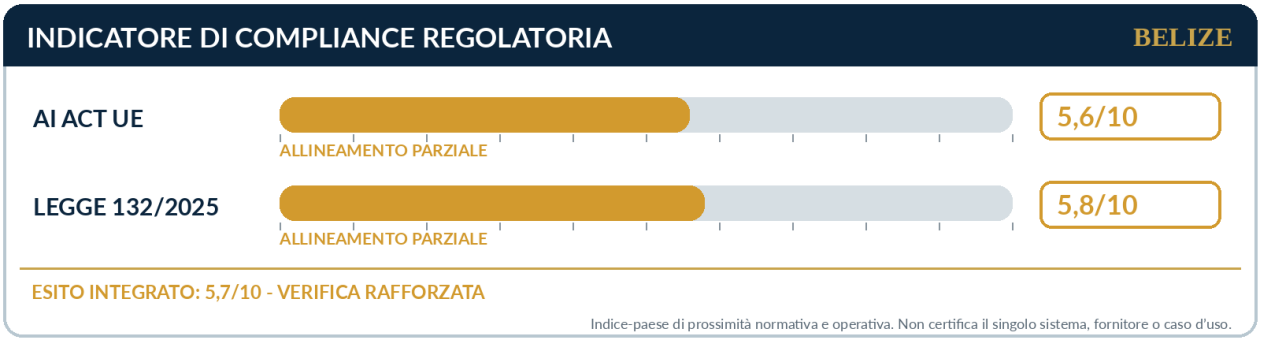
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Belgio: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Belize

Posizione FOTR	75	Area	Americhe	Subregione	Caraibi
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Media	Copertura dati	5/7 famiglie
FOTR / 10	5,9	GCRI / 10	5,0	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Belize, AI Act UE 5,6/10; legge 132/2025 5,8/10; esito integrato 5,7/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Belize non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 87/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,0/10) e indice FOTR (5,9/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. In Belize la trasformazione digitale procede più rapidamente dell'uniformità regolatoria e operativa. Gli investimenti devono essere accompagnati da audit, clausole di uscita e gestione locale del rischio.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	80,0% / 9,8 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	99,6% / 464.560 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	48,7 / 33,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	32,4/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	n.d./100 - rank n.d.	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (87/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,5 / 3,6 / 4,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Belize, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 5/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Belize le evidenze principali sono GTMI 33,9/100, EGDI 48,7/100, GCI 32,4/100. La dimensione più robusta è maturità infrastrutturale (6,6/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,6/10). Sono disponibili 5 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata media. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Belize è 6,6/10. La base statistica rileva utenti Internet pari al 80,0% nel 2024; 9,8 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 99,6% nel 2024; 464.560 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Per Belize non è disponibile un profilo Oxford Insights direttamente attribuibile; l'adozione di IA è quindi valutata attraverso GovTech, servizi online, infrastrutture e fonti qualitative. Il GTMI 2025 è 33,9/100. Il punteggio S2 è 3,6/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Belize è valutata sufficiente ma disomogenea, con S3 pari a 5,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 52,7/100, penetrazione Internet 80,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Belize ottiene S4 5,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Belize, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=5,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Belize è S5 4,2/10. La base ITU registra ITU GCI 32,4/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (87/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,5	Crimini finanziari	5,0
Reti criminali	3,5	Attori incorporati nello Stato	5,5
Attori stranieri	6,0	Attori del settore privato	5,5
Resilienza complessiva	3,6	Cooperazione internazionale	4,5
Politiche e norme nazionali	3,5	Forze dell'ordine	4,0
Antiriciclaggio	2,5	Prevenzione	4,0
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	4,9 - MODERATO

Quadro criminale digitale. Per Belize, l'indice operativo FOTR-CY è 4,9/10, classe moderata. Il mercato dei reati cyber-dipendenti è intermedio (3,5/10), mentre i crimini finanziari sono intermedi (5,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (6,0/10) e attori incorporati nello Stato (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Belize assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Belize, la resilienza complessiva è debole (3,6/10); la cooperazione internazionale è debole (4,5/10), le politiche e norme nazionali sono deboli (3,5/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 2,5/10, prevenzione 4,0/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Belize, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Belize. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Belize, In Belize le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Belize, Il livello governativo di Belize presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Belize, Sul piano militare e dual-use, Belize mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Belize, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Belize, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,7/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,6	3,6	5,4	5,3	4,2	5,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,7	5,9	5,9	6,1	5,9	5,7

Il GCRI di Belize è 5,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,9/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,1/10), mentre il più basso è Compatibilità giuridica (5,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,9/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Belize, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Belize, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Belize, Dal punto di vista italiano, Belize rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Belize è indicata una cooperazione selettiva, coerente con il FOTR di 5,9/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Compatibilità giuridica a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

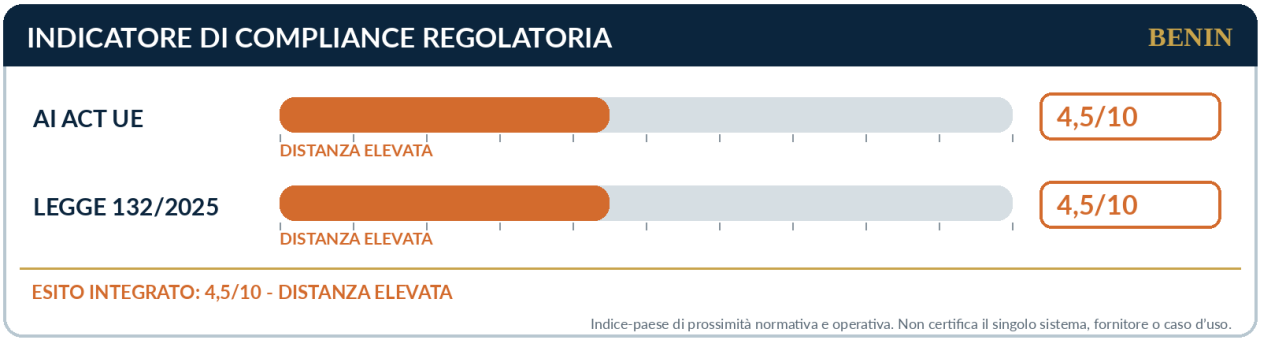
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Belize: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Media con copertura 5/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Benin

Posizione FOTR	144	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,5	GCRI / 10	4,9	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Benin, AI Act UE 4,5/10; legge 132/2025 4,5/10; esito integrato 4,5/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Benin è stato membro delle nazioni unite collocato in Africa occidentale. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 61/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (4,9/10) e indice FOTR (4,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per Benin non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	34,0% / 0,3 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	59,0% / 20 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	45,8 / 72,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	91,5/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	45,7/100 - rank 90	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (61/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 3,8 / 5,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Benin, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Benin le evidenze principali sono GTMI 72,3/100, EGDI 45,8/100, GCI 91,5/100, AI readiness 45,7/100. La dimensione più robusta è postura di sicurezza cyber (7,4/10), mentre la criticità relativa riguarda maturità infrastrutturale (3,5/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Benin è 3,5/10. La base statistica rileva utenti Internet pari al 34,0% nel 2024; 0,3 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 59,0% nel 2024; 20 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Benin al posto 90 con un valore medio di 45,7/100; il pilastro migliore è adozione pubblica (63,0/100), quello più debole è sviluppo e diffusione (26,9/100). Il GTMI 2025 è 72,3/100. Il punteggio S2 è 5,0/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Benin è valutata fragile, con S3 pari a 3,9/10. Le evidenze disponibili comprendono indice UN di capitale umano 37,1/100, sviluppo e diffusione dell'IA 26,9/100, penetrazione Internet 34,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Benin ottiene S4 4,8/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Benin, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,8/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Benin è S5 7,4/10. La base ITU registra ITU GCI 91,5/100, Tier 2 - avanzato; il pilastro relativamente più debole è cooperazione (14,3/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (61/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	6,0
Reti criminali	6,0	Attori incorporati nello Stato	6,0
Attori stranieri	8,0	Attori del settore privato	4,5
Resilienza complessiva	3,8	Cooperazione internazionale	4,5
Politiche e norme nazionali	3,0	Forze dell'ordine	4,0
Antiriciclaggio	4,5	Prevenzione	3,0
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	5,4 - SIGNIFICATIVO

Quadro criminale digitale. Per Benin, l'indice operativo FOTR-CY è 5,4/10, classe significativa. Il mercato dei reati cyber-dipendenti è limitato o poco osservabile (3,0/10), mentre i crimini finanziari sono elevati (6,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (8,0/10) e reti criminali (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Benin assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Benin, la resilienza complessiva è debole (3,8/10); la cooperazione internazionale è debole (4,5/10), le politiche e norme nazionali sono molto deboli (3,0/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 3,0/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Benin, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Benin. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Benin, In Benin le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Benin, Il livello governativo di Benin presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Benin, Sul piano militare e dual-use, Benin mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Benin, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Benin, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,2/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,5	5,0	3,9	4,8	7,4	4,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,8	4,2	4,5	4,7	4,3	4,2

Il GCRI di Benin è 4,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (4,8/10), mentre il più basso è Maturità cyber (4,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Benin, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Benin, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Benin, Dal punto di vista italiano, Benin rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Benin ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.
Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

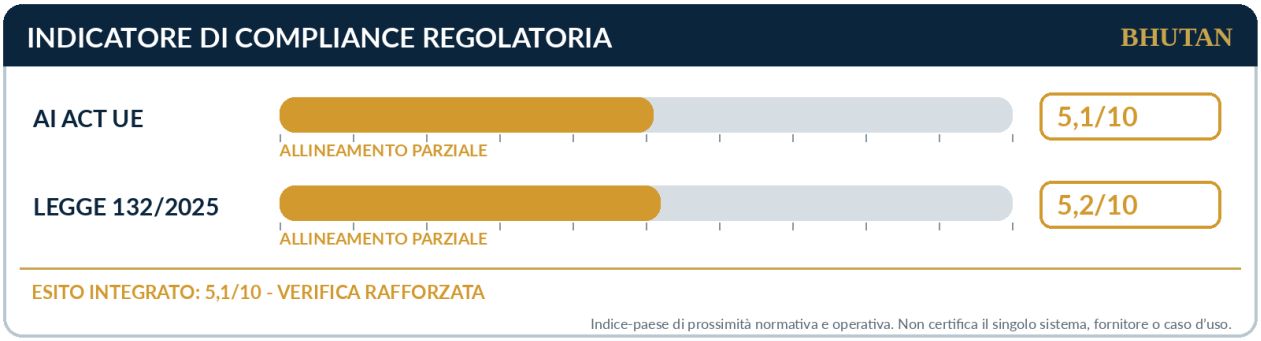
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Benin: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Bhutan

Posizione FOTR	131	Area	Asia	Subregione	Asia meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,1	GCRI / 10	5,6	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Bhutan, AI Act UE 5,1/10; legge 132/2025 5,2/10; esito integrato 5,1/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Asia, Bhutan presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 69/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,6/10) e indice FOTR (5,1/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Bhutan presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	91,3% / 2,9 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 1.339 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	65,1 / 81,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	60,6/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	39,1/100 - rank 101	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (69/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 4,7 / 3,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Bhutan, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Bhutan le evidenze principali sono GTMI 81,4/100, EGDI 65,1/100, GCI 60,6/100, AI readiness 39,1/100. La dimensione più robusta è maturità infrastrutturale (7,1/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (4,7/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Bhutan è 7,1/10. La base statistica rileva utenti Internet pari al 91,3% nel 2024; 2,9 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 1.339 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Bhutan al posto 101 con un valore medio di 39,1/100; il pilastro migliore è adozione pubblica (73,1/100), quello più debole è politiche pubbliche (12,0/100). Il GTMI 2025 è 81,4/100. Il punteggio S2 è 5,0/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Bhutan è valutata fragile, con S3 pari a 4,7/10. Le evidenze disponibili comprendono indice UN di capitale umano 54,8/100, sviluppo e diffusione dell'IA 28,2/100, penetrazione Internet 91,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Bhutan ottiene S4 5,2/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Bhutan, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo societario e

subfornitura. L'impatto sulla valutazione è misurato da S4=5,2/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Bhutan è S5 5,8/10. La base ITU registra ITU GCI 60,6/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è cooperazione (7,2/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (69/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	3,5
Reti criminali	4,5	Attori incorporati nello Stato	3,0
Attori stranieri	4,0	Attori del settore privato	3,0
Resilienza complessiva	4,7	Cooperazione internazionale	5,5
Politiche e norme nazionali	5,0	Forze dell'ordine	5,0
Antiriciclaggio	4,5	Prevenzione	4,0
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	3,9 - MODERATO

Quadro criminale digitale. Per Bhutan, l'indice operativo FOTR-CY è 3,9/10, classe moderata. Il mercato dei reati cyber-dipendenti è limitato o poco osservabile (3,0/10), mentre i crimini finanziari sono intermedi (3,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (4,5/10) e attori stranieri (4,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Bhutan assumono particolare rilevanza compromissione delle caselle di posta aziendale, frodi da call center, abuso di portafogli digitali mobili, identità sintetiche, ransomware, phishing bancario e triangolazioni transfrontaliere dei proventi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Bhutan, la resilienza complessiva è debole (4,7/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 4,0/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Bhutan, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Bhutan. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Bhutan, In Bhutan le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Bhutan, Il livello governativo di Bhutan presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Bhutan, Sul piano militare e dual-use, Bhutan mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Bhutan, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Bhutan, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,5/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,1	5,0	4,7	5,2	5,8	5,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,5	5,7	4,7	5,0	5,1	4,5

Il GCRI di Bhutan è 5,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,1/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Maturità cyber (5,7/10), mentre il più basso è Trasferibilità dati (4,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 5,1/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Bhutan, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Bhutan, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Bhutan, Dal punto di vista italiano, Bhutan rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Bhutan è indicata una cooperazione selettiva, coerente con il FOTR di 5,1/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

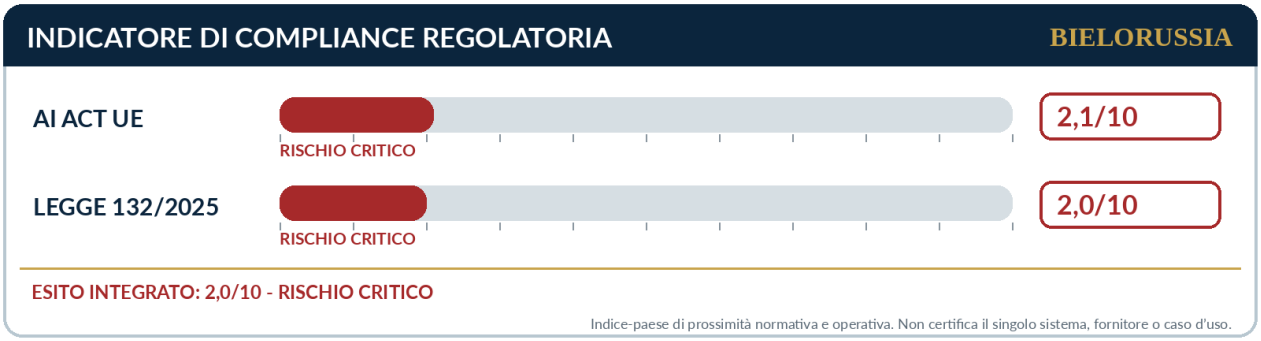
- Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
- Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.
- Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.
- Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Bhutan: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Bielorussia

Posizione FOTR	191	Area	Europa	Subregione	Europa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	1,8	GCRI / 10	5,5	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Bielorussia, AI Act UE 2,1/10; legge 132/2025 2,0/10; esito integrato 2,0/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Bielorussia, situato in Europa orientale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La prossimità europea può ridurre i costi operativi, ma non sostituisce la verifica dell'allineamento al GDPR, delle autorità indipendenti e della reale origine dei servizi cloud. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina, Russia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 7/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (5,5/10) è superiore al punteggio FOTR (1,8/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Il rapporto digitale con Bielorussia deve essere considerato eccezionale e ad alta esposizione. Sono necessari screening sanzionatori, autorizzazioni, segregazione completa e impossibilità tecnica di accedere ai dati in chiaro.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	94,3% / 36,3 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 12.730 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	74,4 / 79,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	61,5/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	31,0/100 - rank 121	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	20/100 - Non libero / Non libero (7/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,0 / 3,1 / 7,3	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Bielorussia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Bielorussia le evidenze principali sono GTMI 79,7/100, EGDI 74,4/100, GCI 61,5/100, AI readiness 31,0/100. La dimensione più robusta è maturità infrastrutturale (9,2/10), mentre la criticità relativa riguarda postura di sicurezza cyber (4,2/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Bielorussia è 9,2/10. La base statistica rileva utenti Internet pari al 94,3% nel 2024; 36,3 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 12.730 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Bielorussia al posto 121 con un valore medio di 31,0/100; il pilastro migliore è infrastrutture IA (45,3/100), quello più debole è politiche pubbliche (12,0/100). Il GTMI 2025 è 79,7/100. Il punteggio S2 è 4,5/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Bielorussia è valutata fragile, con S3 pari a 4,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 74,2/100, sviluppo e diffusione dell'IA 24,6/100, penetrazione Internet 94,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Bielorussia ottiene S4 4,7/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina, Russia; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Bielorussia, Prevalenza russa, con crescente presenza cinese e capacità domestiche selettive. L'impatto sulla valutazione è misurato da S4=4,7/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Bielorussia è S5 4,2/10. La base ITU registra ITU GCI 61,5/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (2,8/20). Freedom on the Net è 20/100 - Non libero, mentre Freedom in the World è Non libero (7/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Legge sulla protezione dei dati personali, localizzazione e ampi poteri statali; sanzioni e limitata indipendenza dei controlli riducono fortemente l'affidabilità.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,0	Crimini finanziari	8,0
Reti criminali	5,0	Attori incorporati nello Stato	9,0
Attori stranieri	6,5	Attori del settore privato	7,5
Resilienza complessiva	3,1	Cooperazione internazionale	3,0
Politiche e norme nazionali	3,5	Forze dell'ordine	3,0
Antiriciclaggio	4,0	Prevenzione	4,0
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	7,3 - ALTO

Sintesi del rischio cybercrime. Bielorussia presenta un'esposizione stimata alta (7,3/10): reati cyber-dipendenti 7,0/10, crimini finanziari 8,0/10 e resilienza 3,1/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e attori del settore privato (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Bielorussia assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Bielorussia, la resilienza complessiva è molto debole (3,1/10); la cooperazione internazionale è molto debole (3,0/10), le politiche e norme nazionali sono deboli (3,5/10) e la capacità delle forze dell'ordine è molto debole (3,0/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Bielorussia, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; blocco di hosting e ASN ad alta reputazione negativa, ricerca proattiva delle minacce su malware sottrattori di informazioni e controllo dei canali RDP/VPN; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Bielorussia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Bielorussia, In Bielorussia le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Bielorussia, Il livello governativo di Bielorussia presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Bielorussia, Sul piano militare e dual-use, Bielorussia mostra forte integrazione o dipendenza dall'ecosistema russo, inclusi sistemi di comando, comunicazione e sicurezza. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Bielorussia, Legge sulla protezione dei dati personali, localizzazione e ampi poteri statali; sanzioni e limitata indipendenza dei controlli riducono fortemente l'affidabilità. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Bielorussia, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 0,1/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,2	4,5	4,8	4,7	4,2	5,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
2,4	3,4	1,0	0,6	3,0	0,1

Il GCRI di Bielorussia è 5,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 1,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (3,4/10), mentre il più basso è Trasferibilità dati (0,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Alto	Estremo	Estremo	Estremo

La matrice applica il FOTR di 1,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Bielorussia, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Bielorussia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Bielorussia, Dal punto di vista italiano, Bielorussia rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Bielorussia, il FOTR di 1,8/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

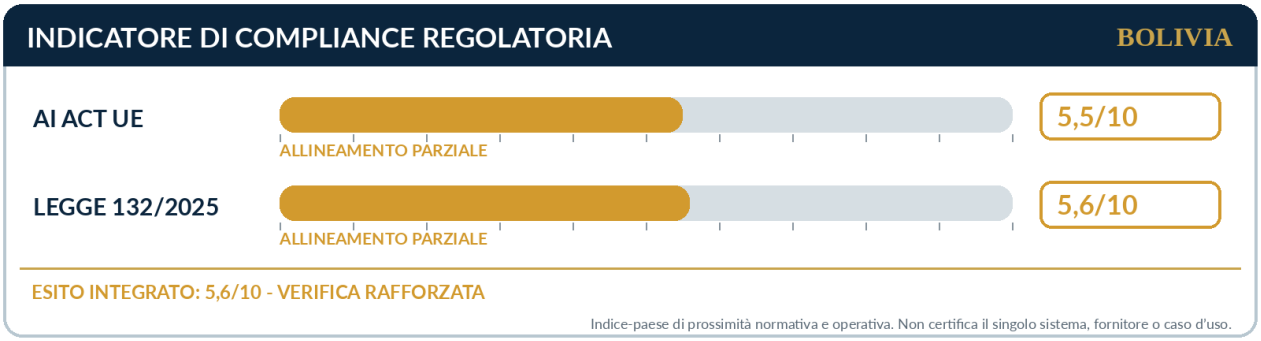
Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.
Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.
Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Bielorussia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Bolivia

Posizione FOTR	94	Area	Americhe	Subregione	America meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,7	GCRI / 10	5,0	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Bolivia, AI Act UE 5,5/10; legge 132/2025 5,6/10; esito integrato 5,6/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Bolivia non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 69/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,0/10) e indice FOTR (5,7/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Bolivia dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	79,7% / 12,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	96,6% / 364 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	66,5 / 57,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	43,0/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	26,9/100 - rank 139	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (69/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 4,6 / 5,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Bolivia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Bolivia le evidenze principali sono GTMI 57,2/100, EGDI 66,5/100, GCI 43,0/100, AI readiness 26,9/100. La dimensione più robusta è maturità infrastrutturale (6,6/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,7/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Bolivia è 6,6/10. La base statistica rileva utenti Internet pari al 79,7% nel 2024; 12,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 96,6% nel 2024; 364 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Bolivia al posto 139 con un valore medio di 26,9/100; il pilastro migliore è adozione pubblica (45,0/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 57,2/100. Il punteggio S2 è 3,7/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Bolivia è valutata sufficiente ma disomogenea, con S3 pari a 5,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 68,8/100, sviluppo e diffusione dell'IA 13,6/100, penetrazione Internet 79,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Bolivia ottiene S4 5,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Bolivia, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=5,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Bolivia è S5 4,8/10. La base ITU registra ITU GCI 43,0/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è organizzazione (4,7/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (69/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	5,0
Reti criminali	5,0	Attori incorporati nello Stato	6,5
Attori stranieri	5,5	Attori del settore privato	5,0
Resilienza complessiva	4,6	Cooperazione internazionale	5,0
Politiche e norme nazionali	6,0	Forze dell'ordine	4,5
Antiriciclaggio	4,5	Prevenzione	5,5
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	5,1 - SIGNIFICATIVO

Quadro criminale digitale. Per Bolivia, l'indice operativo FOTR-CY è 5,1/10, classe significativa. Il mercato dei reati cyber-dipendenti è intermedio (4,5/10), mentre i crimini finanziari sono intermedi (5,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (6,5/10) e attori stranieri (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Bolivia assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Bolivia, la resilienza complessiva è debole (4,6/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 5,5/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Bolivia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Bolivia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Bolivia, In Bolivia le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Bolivia, Il livello governativo di Bolivia presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Bolivia, Sul piano militare e dual-use, Bolivia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Bolivia, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Bolivia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,7/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,6	3,7	5,0	5,1	4,8	5,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,8	5,8	5,5	5,9	5,5	5,7

Il GCRI di Bolivia è 5,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,9/10), mentre il più basso è Trasparenza istituzionale (5,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Bolivia, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Bolivia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Bolivia, Dal punto di vista italiano, Bolivia rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Bolivia è indicata una cooperazione selettiva, coerente con il FOTR di 5,7/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasparenza istituzionale a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

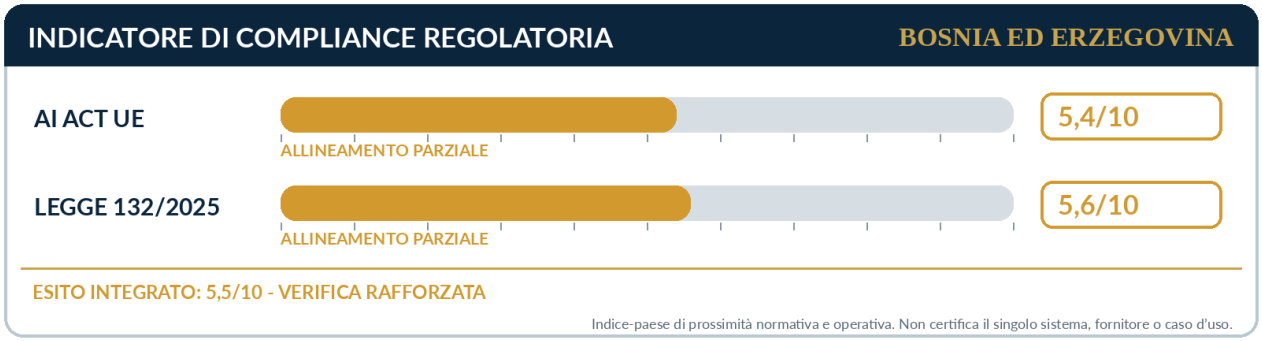
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Bolivia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Bosnia ed Erzegovina

Posizione FOTR	107	Area	Europa	Subregione	Europa sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,6	GCRI / 10	5,2	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Bosnia ed Erzegovina, AI Act UE 5,4/10; legge 132/2025 5,6/10; esito integrato 5,5/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Bosnia ed Erzegovina è stato membro delle nazioni unite collocato in Europa sud-orientale. La prossimità europea può ridurre i costi operativi, ma non sostituisce la verifica dell'allineamento al GDPR, delle autorità indipendenti e della reale origine dei servizi cloud. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Cina, Russia, Turchia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 54/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,2/10) e indice FOTR (5,6/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. In Bosnia ed Erzegovina la trasformazione digitale procede più rapidamente dell'uniformità regolatoria e operativa. Gli investimenti devono essere accompagnati da audit, clausole di uscita e gestione locale del rischio.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	86,1% / 29,4 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 5.554 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	63,3 / 43,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	33,8/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	35,2/100 - rank 114	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (54/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,0 / 3,9 / 5,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Bosnia ed Erzegovina, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Bosnia ed Erzegovina le evidenze principali sono GTMI 43,3/100, EGDI 63,3/100, GCI 33,8/100, AI readiness 35,2/100. La dimensione più robusta è maturità infrastrutturale (8,1/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Bosnia ed Erzegovina è 8,1/10. La base statistica rileva utenti Internet pari al 86,1% nel 2024; 29,4 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 5.554 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Bosnia ed Erzegovina al posto 114 con un valore medio di 35,2/100; il pilastro migliore è adozione pubblica (51,8/100), quello più debole è politiche pubbliche (19,0/100). Il GTMI 2025 è 43,3/100. Il punteggio S2 è 3,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Bosnia ed Erzegovina è valutata fragile, con S3 pari a 4,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 62,2/100, sviluppo e diffusione dell'IA 19,4/100, penetrazione Internet 86,1%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Bosnia ed Erzegovina ottiene S4 5,4/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Cina, Russia, Turchia; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Bosnia ed Erzegovina, Mercato multi-fornitore tra Unione europea, Stati Uniti, Turchia, Cina e, in alcuni segmenti, Russia; il peso relativo varia tra pubblico, telecomunicazioni e difesa. L'impatto sulla

valutazione è misurato da S4=5,4/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Bosnia ed Erzegovina è S5 4,0/10. La base ITU registra ITU GCI 33,8/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (2,7/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (54/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Quadro nazionale di protezione dati e cybersicurezza in progressivo allineamento all'acquis dell'Unione europea; la distanza tra legge formale, vigilanza e prassi deve essere verificata nel settore interessato.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,0	Crimini finanziari	6,5
Reti criminali	6,0	Attori incorporati nello Stato	8,0
Attori stranieri	7,0	Attori del settore privato	6,5
Resilienza complessiva	3,9	Cooperazione internazionale	6,0
Politiche e norme nazionali	4,0	Forze dell'ordine	3,5
Antiriciclaggio	3,5	Prevenzione	4,5
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	5,8 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Bosnia ed Erzegovina restituisce un rischio FOTR-CY di 5,8/10 (significativo). La componente cyber-dipendente vale 4,0/10 e quella finanziaria 6,5/10; la risposta sistemica è valutata debole, con resilienza media di 3,9/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e attori stranieri (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Bosnia ed Erzegovina assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Bosnia ed Erzegovina, la resilienza complessiva è debole (3,9/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono deboli (4,0/10) e la capacità delle forze dell'ordine è debole (3,5/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 4,5/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Bosnia ed Erzegovina, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Bosnia ed Erzegovina. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Bosnia ed Erzegovina, In Bosnia ed Erzegovina le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora

visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Bosnia ed Erzegovina, Il livello governativo di Bosnia ed Erzegovina presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Bosnia ed Erzegovina, Sul piano militare e dual-use, Bosnia ed Erzegovina mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Bosnia ed Erzegovina, Quadro nazionale di protezione dati e cybersicurezza in progressivo allineamento all'acquis dell'Unione europea; la distanza tra legge formale, vigilanza e prassi deve essere verificata nel settore interessato. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Bosnia ed Erzegovina, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,3/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,1	3,9	4,8	5,4	4,0	5,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,2	5,2	5,0	6,7	5,2	5,3

Il GCRI di Bosnia ed Erzegovina è 5,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,7/10), mentre il più basso è Trasparenza istituzionale (5,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio-alto	Medio

La matrice applica il FOTR di 5,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Bosnia ed Erzegovina, 1 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Pubblica amministrazione. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Bosnia ed Erzegovina, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Bosnia ed Erzegovina, Dal punto di vista italiano, Bosnia ed Erzegovina rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Bosnia ed Erzegovina è indicata una cooperazione selettiva, coerente con il FOTR di 5,6/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Pubblica amministrazione a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

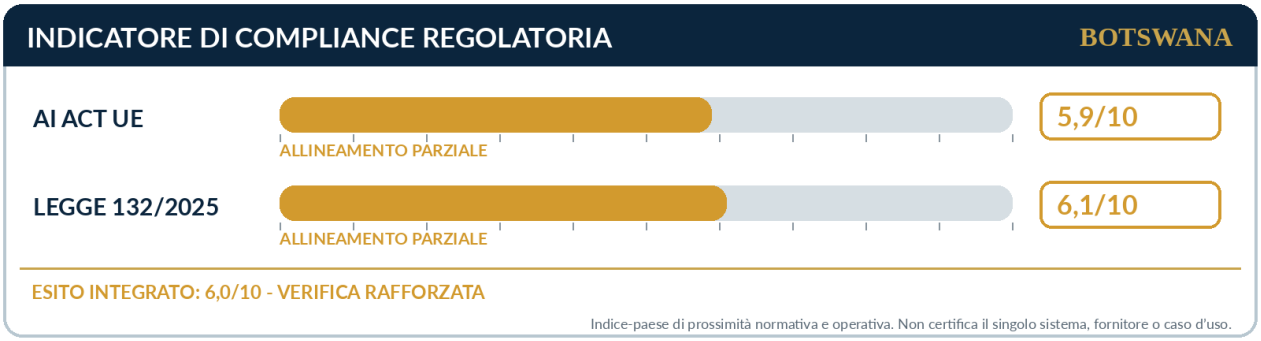
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Bosnia ed Erzegovina: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Botswana

Posizione FOTR	70	Area	Africa	Subregione	Africa australe
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	6,1	GCRI / 10	5,5	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Botswana, AI Act UE 5,9/10; legge 132/2025 6,1/10; esito integrato 6,0/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Botswana presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 75/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,5/10) e indice FOTR (6,1/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il quadro di Botswana è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	57,5% / 7,4 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	80,2% / 471 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	61,2 / 46,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	78,6/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	36,5/100 - rank 109	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (75/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 5,4 / 5,3	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Botswana, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Botswana le evidenze principali sono GTMI 46,9/100, EGDI 61,2/100, GCI 78,6/100, AI readiness 36,5/100. La dimensione più robusta è postura di sicurezza cyber (7,2/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Botswana è 6,3/10. La base statistica rileva utenti Internet pari al 57,5% nel 2024; 7,4 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 80,2% nel 2024; 471 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Botswana al posto 109 con un valore medio di 36,5/100; il pilastro migliore è governance (60,6/100), quello più debole è politiche pubbliche (19,5/100). Il GTMI 2025 è 46,9/100. Il punteggio S2 è 3,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Botswana è valutata sufficiente ma disomogenea, con S3 pari a 5,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 57,2/100, sviluppo e diffusione dell'IA 27,8/100, penetrazione Internet 57,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Botswana ottiene S4 4,9/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Botswana, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,9/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Botswana è S5 7,2/10. La base ITU registra ITU GCI 78,6/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (13,3/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (75/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Data Protection Act e Cybercrime and Computer Related Crimes Act; capacità istituzionale discreta ma mercato limitato.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	6,0
Reti criminali	5,5	Attori incorporati nello Stato	4,5
Attori stranieri	5,5	Attori del settore privato	4,0
Resilienza complessiva	5,4	Cooperazione internazionale	7,5
Politiche e norme nazionali	7,0	Forze dell'ordine	5,0
Antiriciclaggio	5,5	Prevenzione	4,5
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	5,3 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (5,5/10), criminalità finanziaria (6,0/10) e resilienza (5,4/10) colloca Botswana in una fascia di rischio significativo, pari a 5,3/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (5,5/10) e attori stranieri (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Botswana assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Botswana, la resilienza complessiva è debole (5,4/10); la cooperazione internazionale è robusta (7,5/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 4,5/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Botswana, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Botswana. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Botswana, In Botswana le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Botswana, Il livello governativo di Botswana presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Botswana, Sul piano militare e dual-use, Botswana mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Botswana, Data Protection Act e Cybercrime and Computer Related Crimes Act; capacità istituzionale discreta ma mercato limitato. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Botswana, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 6,0/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,3	3,9	5,1	4,9	7,2	5,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,2	6,1	6,1	6,7	5,6	6,0

Il GCRI di Botswana è 5,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,1/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,7/10), mentre il più basso è Supply chain (5,6/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,1/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Botswana, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Botswana, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Botswana, Dal punto di vista italiano, Botswana rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Botswana è indicata una cooperazione selettiva, coerente con il FOTR di 6,1/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Supply chain a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

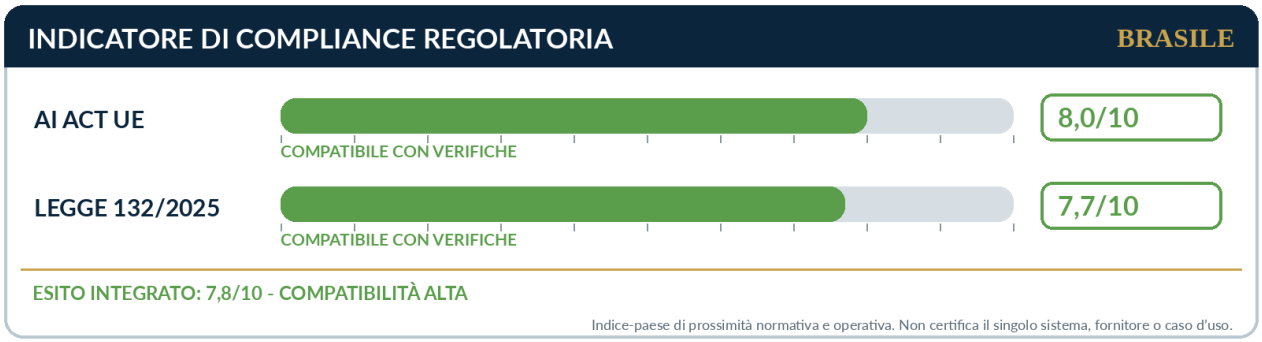
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Botswana: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Brasile

Posizione FOTR	43	Area	Americhe	Subregione	America meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	7,8	GCRI / 10	7,5	Classe operativa	Affidabilità favorevole ma condizionata

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Brasile, AI Act UE 8,0/10; legge 132/2025 7,7/10; esito integrato 7,8/10, classe «Compatibile con verifiche». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Prima dell'ingaggio occorre una analisi degli scostamenti mirata su trasparenza, governance dei dati, rappresentanza nell'UE, audit e rimedi contrattuali.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Brasile, situato in America meridionale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La partecipazione al coordinamento BRICS segnala una strategia di autonomia e diversificazione rispetto agli ecosistemi occidentali, con relazioni tecnologiche più intense verso Cina, Russia o altri poli emergenti. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 73/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,5/10) e indice FOTR (7,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Mercato latinoamericano centrale, disciplina LGPD matura e adeguatezza UE dal 2026; rimangono differenze di capacità tra settori e territori.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	84,5% / 24,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	99,8% / 6.941 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	84,0 / 98,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	96,4/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	73,5/100 - rank 22	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	65/100 - Parzialmente libero / Libero (73/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	8,0 / 5,0 / 6,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Brasile, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Brasile le evidenze principali sono GTMI 98,6/100, EGDI 84,0/100, GCI 96,4/100, AI readiness 73,5/100. La dimensione più robusta è postura di sicurezza cyber (8,4/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,3/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Brasile è 8,0/10. La base statistica rileva utenti Internet pari al 84,5% nel 2024; 24,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 99,8% nel 2024; 6.941 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Brasile al posto 22 con un valore medio di 73,5/100; il pilastro migliore è adozione pubblica (94,8/100), quello più debole è sviluppo e diffusione (46,6/100). Il GTMI 2025 è 98,6/100. Il punteggio S2 è 8,0/10 e indica una capacità elevata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Brasile è valutata sufficiente ma disomogenea, con S3 pari a 7,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 80,8/100, sviluppo e diffusione dell'IA 46,6/100, penetrazione Internet 84,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Brasile ottiene S4 6,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Brasile, Fornitori nazionali, statunitensi, europei e cinesi; forte mercato cloud e telecom multi-origine. L'impatto sulla valutazione è misurato da S4=6,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Brasile è S5 8,4/10. La base ITU registra ITU GCI 96,4/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è organizzazione (17,3/20). Freedom on the Net è 65/100 - Parzialmente libero, mentre Freedom in the World è Libero (73/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Lei Geral de Proteção de Dados, Marco Civil da Internet e poteri dell'ANPD; decisione UE di adeguatezza del 26 gennaio 2026.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	8,0	Crimini finanziari	8,0
Reti criminali	7,0	Attori incorporati nello Stato	8,5
Attori stranieri	4,0	Attori del settore privato	7,0
Resilienza complessiva	5,0	Cooperazione internazionale	7,5
Politiche e norme nazionali	5,0	Forze dell'ordine	4,0
Antiriciclaggio	6,0	Prevenzione	4,0
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	6,8 - ALTO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (8,0/10), criminalità finanziaria (8,0/10) e resilienza (5,0/10) colloca Brasile in una fascia di rischio alto, pari a 6,8/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,5/10) e reti criminali (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Brasile assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Brasile, la resilienza complessiva è debole (5,0/10); la cooperazione internazionale è robusta (7,5/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Brasile, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Brasile. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Brasile, In Brasile le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. La superficie di rischio

comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Brasile, Il livello governativo di Brasile presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Brasile, Sul piano militare e dual-use, Brasile mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Brasile, Lei Geral de Proteção de Dados, Marco Civil da Internet e poteri dell'ANPD; decisione UE di adeguatezza del 26 gennaio 2026. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Brasile, La decisione UE di adeguatezza del 26 gennaio 2026 consente il trasferimento senza ulteriori garanzie ai sensi del capo V GDPR, ferma la necessità di verificare finalità, sicurezza, destinatari e trasferimenti successivi. La componente FOTR di trasferibilità è 9,7/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,0	8,0	7,0	6,3	8,4	7,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,1	8,0	6,9	6,9	7,4	9,7

Il GCRI di Brasile è 7,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 7,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,7/10), mentre il più basso è Trasparenza istituzionale (6,9/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 7,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Brasile, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Brasile, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Brasile, Dal punto di vista italiano, Brasile rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Brasile è favorevole ma condizionata: il valore FOTR di 7,8/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Trasparenza istituzionale.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

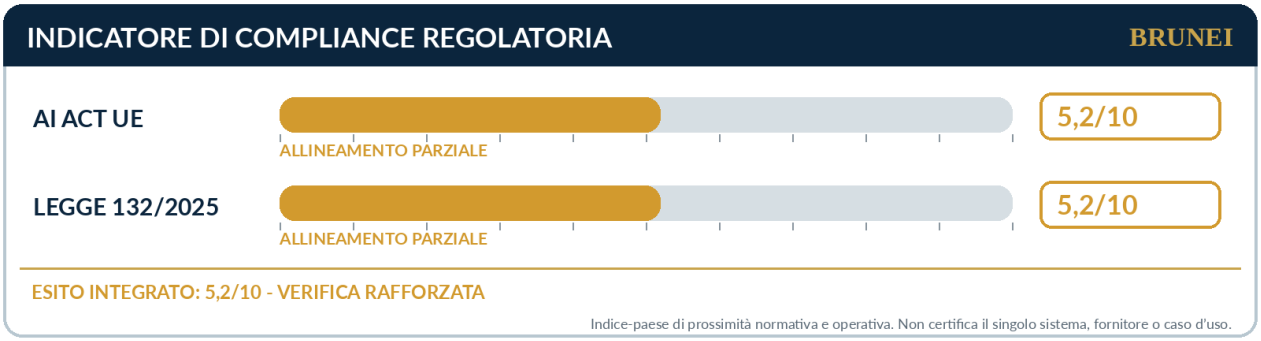
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Brasile: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Brunei

Posizione FOTR	125	Area	Asia	Subregione	Asia sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,2	GCRI / 10	6,0	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Brunei, AI Act UE 5,2/10; legge 132/2025 5,2/10; esito integrato 5,2/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Brunei non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 27/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,0/10) e indice FOTR (5,2/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per Brunei non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	96,3% / 21,2 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 16.129 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	75,5 / 53,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	70,4/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	41,0/100 - rank 97	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (27/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,0 / 4,6 / 4,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Brunei, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Brunei le evidenze principali sono GTMI 53,6/100, EGDI 75,5/100, GCI 70,4/100, AI readiness 41,0/100. La dimensione più robusta è maturità infrastrutturale (8,8/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,6/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Brunei è 8,8/10. La base statistica rileva utenti Internet pari al 96,3% nel 2024; 21,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 16.129 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Brunei al posto 97 con un valore medio di 41,0/100; il pilastro migliore è adozione pubblica (65,1/100), quello più debole è sviluppo e diffusione (25,4/100). Il GTMI 2025 è 53,6/100. Il punteggio S2 è 4,6/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Brunei è valutata sufficiente ma disomogenea, con S3 pari a 5,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 69,9/100, sviluppo e diffusione dell'IA 25,4/100, penetrazione Internet 96,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Brunei ottiene S4 5,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Brunei, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo societario e

subfornitura. L'impatto sulla valutazione è misurato da S4=5,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Brunei è S5 6,5/10. La base ITU registra ITU GCI 70,4/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (10,8/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (27/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,0	Crimini finanziari	4,5
Reti criminali	2,0	Attori incorporati nello Stato	3,0
Attori stranieri	4,0	Attori del settore privato	3,0
Resilienza complessiva	4,6	Cooperazione internazionale	5,0
Politiche e norme nazionali	4,5	Forze dell'ordine	5,5
Antiriciclaggio	5,5	Prevenzione	5,0
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	4,1 - MODERATO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (4,0/10), criminalità finanziaria (4,5/10) e resilienza (4,6/10) colloca Brunei in una fascia di rischio moderato, pari a 4,1/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (4,0/10) e attori incorporati nello Stato (3,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Brunei assumono particolare rilevanza centri organizzati di truffa, frodi d'investimento e sentimentali, phishing multicanale, batterie di schede SIM, conti prestanome, riciclaggio in cripto-attività e compromissione di servizi esternalizzati. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Brunei, la resilienza complessiva è debole (4,6/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono deboli (4,5/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 5,0/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Brunei, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; controllo della filiera contro esposizione a complessi organizzati per truffe telematiche, call center coercitivi e conti prestanome; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Brunei. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Brunei, In Brunei le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Brunei, Il livello governativo di Brunei presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Brunei, Sul piano militare e dual-use, Brunei mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Brunei, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Brunei, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,9/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,8	4,6	5,1	5,1	6,5	6,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,2	5,6	5,1	5,3	5,3	4,9

Il GCRI di Brunei è 6,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (5,6/10), mentre il più basso è Trasferibilità dati (4,9/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 5,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Brunei, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Brunei, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Brunei, Dal punto di vista italiano, Brunei rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Brunei è indicata una cooperazione selettiva, coerente con il FOTR di 5,2/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.
Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

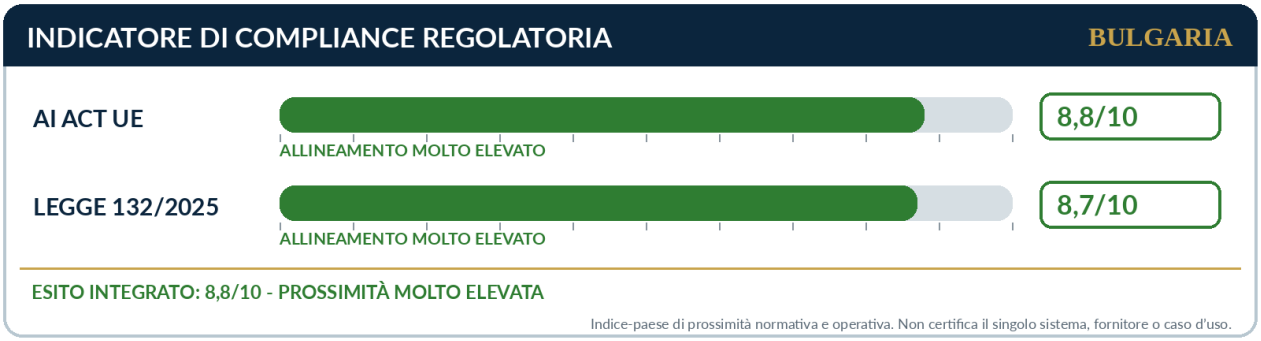
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Brunei: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Bulgaria

Posizione FOTR	38	Area	Europa	Subregione	Europa sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,0	GCRI / 10	7,0	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Bulgaria, AI Act UE 8,8/10; legge 132/2025 8,7/10; esito integrato 8,8/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Bulgaria è stato membro delle nazioni unite collocato in Europa sud-orientale. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 74/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (8,0/10) supera il GCRI tecnico (7,0/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Bulgaria combina buona maturità tecnologica e relativa prevedibilità normativa. Il livello di rischio aumenta nei progetti che coinvolgono dati sanitari, identità, infrastrutture critiche o ricerca strategica.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	82,4% / 37,0 per 100	2024/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 50.751 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	81,5 / 76,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	74,6/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	59,6/100 - rank 59	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (74/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,0 / 5,3 / 5,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Bulgaria, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Bulgaria le evidenze principali sono GTMI 76,2/100, EGDI 81,5/100, GCI 74,6/100, AI readiness 59,6/100. La dimensione più robusta è maturità infrastrutturale (9,1/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,7/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Bulgaria è 9,1/10. La base statistica rileva utenti Internet pari al 82,4% nel 2024; 37,0 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 100,0% nel 2024; 50.751 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Bulgaria al posto 59 con un valore medio di 59,6/100; il pilastro migliore è governance (71,2/100), quello più debole è sviluppo e diffusione (39,8/100). Il GTMI 2025 è 76,2/100. Il punteggio S2 è 6,4/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Bulgaria è valutata sufficiente ma disomogenea, con S3 pari a 6,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 75,4/100, sviluppo e diffusione dell'IA 39,8/100, penetrazione Internet 82,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Bulgaria ottiene S4 5,7/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Bulgaria, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=5,7/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Bulgaria è S5 7,4/10. La base ITU registra ITU GCI 74,6/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è cooperazione (11,1/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (74/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, Personal Data Protection Act e disciplina nazionale NIS2; applicazione del quadro digitale UE.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,0	Crimini finanziari	7,0
Reti criminali	6,0	Attori incorporati nello Stato	7,5
Attori stranieri	5,0	Attori del settore privato	5,5
Resilienza complessiva	5,3	Cooperazione internazionale	6,5
Politiche e norme nazionali	6,0	Forze dell'ordine	5,0
Antiriciclaggio	5,0	Prevenzione	5,0
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	5,9 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Bulgaria restituisce un rischio FOTR-CY di 5,9/10 (significativo). La componente cyber-dipendente vale 6,0/10 e quella finanziaria 7,0/10; la risposta sistemica è valutata debole, con resilienza media di 5,3/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,5/10) e reti criminali (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Bulgaria assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Bulgaria, la resilienza complessiva è debole (5,3/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 5,0/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Bulgaria, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Bulgaria. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Bulgaria, In Bulgaria le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Bulgaria, Il livello governativo di Bulgaria presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Bulgaria, Sul piano militare e dual-use, Bulgaria mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Bulgaria, GDPR, Personal Data Protection Act e disciplina nazionale NIS2; applicazione del quadro digitale UE. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Bulgaria, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 8,8/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,1	6,4	6,6	5,7	7,4	7,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,7	7,2	7,6	8,7	6,8	8,8

Il GCRI di Bulgaria è 7,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (8,8/10), mentre il più basso è Supply chain (6,8/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Bulgaria, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Bulgaria, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Bulgaria, Dal punto di vista italiano, Bulgaria rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Bulgaria, il FOTR di 8,0/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (6,8/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

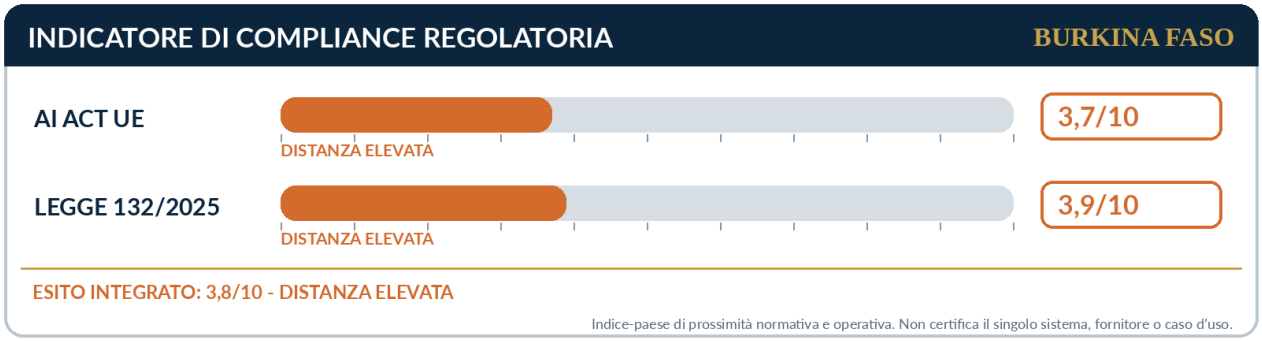
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Bulgaria: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Burkina Faso

Posizione FOTR	183	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	3,7	GCRI / 10	3,3	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Burkina Faso, AI Act UE 3,7/10; legge 132/2025 3,9/10; esito integrato 3,8/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Burkina Faso presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 20/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (3,3/10) e indice FOTR (3,7/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il contesto di Burkina Faso richiede una presunzione prudenziale sfavorevole: anche contratti formalmente corretti possono non compensare carenze nei rimedi, nella continuità o nel controllo della supply chain.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	28,3% / 0,9 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	34,0% / 29 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	28,9 / 43,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	70,2/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	31,4/100 - rank 127	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (20/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 2,9 / 6,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Burkina Faso, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Burkina Faso le evidenze principali sono GTMI 43,3/100, EGDI 28,9/100, GCI 70,2/100, AI readiness 31,4/100. La dimensione più robusta è postura di sicurezza cyber (4,9/10), mentre la criticità relativa riguarda maturità infrastrutturale (2,2/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Burkina Faso è 2,2/10. La base statistica rileva utenti Internet pari al 28,3% nel 2024; 0,9 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 34,0% nel 2024; 29 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Burkina Faso al posto 127 con un valore medio di 31,4/100; il pilastro migliore è adozione pubblica (48,4/100), quello più debole è sviluppo e diffusione (15,0/100). Il GTMI 2025 è 43,3/100. Il punteggio S2 è 3,3/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Burkina Faso è valutata fragile, con S3 pari a 2,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 16,7/100, sviluppo e diffusione dell'IA 15,0/100, penetrazione Internet 28,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Burkina Faso ottiene S4 3,8/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Burkina Faso, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre

ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=3,8/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Burkina Faso è S5 4,9/10. La base ITU registra ITU GCI 70,2/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (11,6/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (20/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	5,5
Reti criminali	7,0	Attori incorporati nello Stato	7,0
Attori stranieri	6,5	Attori del settore privato	6,0
Resilienza complessiva	2,9	Cooperazione internazionale	3,5
Politiche e norme nazionali	5,5	Forze dell'ordine	3,0
Antiriciclaggio	3,5	Prevenzione	2,0
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	6,2 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Burkina Faso presenta un'esposizione stimata significativa (6,2/10): reati cyber-dipendenti 4,5/10, crimini finanziari 5,5/10 e resilienza 2,9/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (7,0/10) e attori incorporati nello Stato (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Burkina Faso assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Burkina Faso, la resilienza complessiva è molto debole (2,9/10); la cooperazione internazionale è debole (3,5/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è molto debole (3,0/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 2,0/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Burkina Faso, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Burkina Faso. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Burkina Faso, In Burkina Faso le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Burkina Faso, Il livello governativo di Burkina Faso presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Burkina Faso, Sul piano militare e dual-use, Burkina Faso mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Burkina Faso, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Burkina Faso, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 3,0/10 e il rischio sui dati personali è Alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
2,2	3,3	2,4	3,8	4,9	3,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,3	3,1	3,6	5,0	3,4	3,0

Il GCRI di Burkina Faso è 3,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 3,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,0/10), mentre il più basso è Trasferibilità dati (3,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Alto	Alto	Alto	Alto	Alto	Medio-alto

La matrice applica il FOTR di 3,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Burkina Faso, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Burkina Faso, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Burkina Faso, Dal punto di vista italiano, Burkina Faso rientra nella classe «Rischio alto»: cooperazione eccezionale e ad alto controllo, subordinata a assenza di dati sensibili, verifica sanzionatoria, autorizzazioni interne e impossibilità di accesso ai sistemi strategici. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Burkina Faso ricade nella fascia di alto rischio (3,7/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

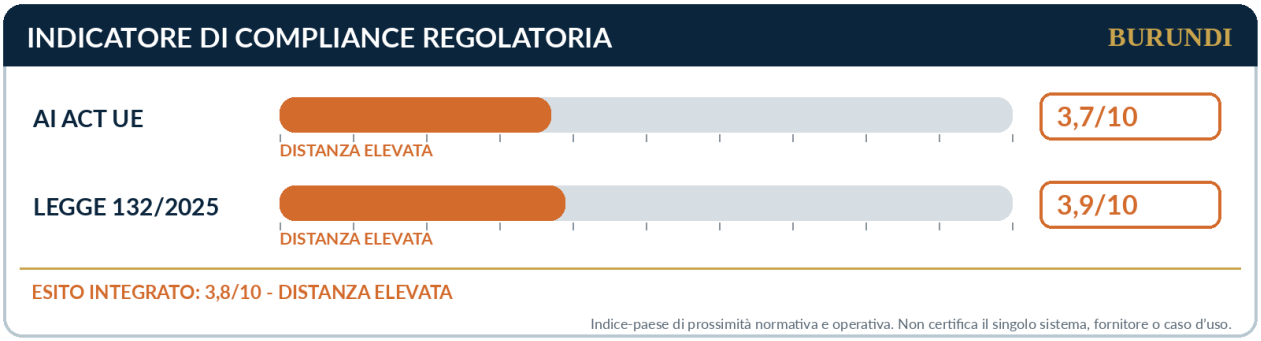
Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.
Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.
Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Burkina Faso: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Burundi

Posizione FOTR	176	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	3,9	GCRI / 10	2,5	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Burundi, AI Act UE 3,7/10; legge 132/2025 3,9/10; esito integrato 3,8/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Burundi, situato in Africa orientale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 13/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (3,9/10) supera il GCRI tecnico (2,5/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il contesto di Burundi richiede una presunzione prudenziale sfavorevole: anche contratti formalmente corretti possono non compensare carenze nei rimedi, nella continuità o nel controllo della supply chain.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	8,6% / 0,0 per 100	2024/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	20,1% / 11 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	24,8 / 41,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	16,8/100 - Tier 5 - capacità iniziali	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	17,5/100 - rank 185	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (13/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	1,5 / 2,3 / 5,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Burundi, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Burundi le evidenze principali sono GTMI 41,3/100, EGDI 24,8/100, GCI 16,8/100, AI readiness 17,5/100. La dimensione più robusta è indipendenza della supply chain (4,0/10), mentre la criticità relativa riguarda maturità infrastrutturale (0,8/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Burundi è 0,8/10. La base statistica rileva utenti Internet pari al 8,6% nel 2024; 0,0 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 20,1% nel 2024; 11 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Burundi al posto 185 con un valore medio di 17,5/100; il pilastro migliore è adozione pubblica (36,4/100), quello più debole è politiche pubbliche (11,5/100). Il GTMI 2025 è 41,3/100. Il punteggio S2 è 2,4/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Burundi è valutata fragile, con S3 pari a 2,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 39,7/100, sviluppo e diffusione dell'IA 12,2/100, penetrazione Internet 8,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Burundi ottiene S4 4,0/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Burundi, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,0/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Burundi è S5 2,3/10. La base ITU registra ITU GCI 16,8/100, Tier 5 - capacità iniziali; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (13/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	1,5	Crimini finanziari	7,5
Reti criminali	4,0	Attori incorporati nello Stato	8,5
Attori stranieri	4,5	Attori del settore privato	6,0
Resilienza complessiva	2,3	Cooperazione internazionale	2,5
Politiche e norme nazionali	3,0	Forze dell'ordine	1,5
Antiriciclaggio	2,5	Prevenzione	3,0
Supporto vittime e testimoni	1,5	Rischio operativo FOTR-CY	5,4 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Burundi il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,4/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 1,5/10; le frodi e i reati finanziari 7,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,5/10) e attori del settore privato (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Burundi assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Burundi, la resilienza complessiva è molto debole (2,3/10); la cooperazione internazionale è molto debole (2,5/10), le politiche e norme nazionali sono molto deboli (3,0/10) e la capacità delle forze dell'ordine è molto debole (1,5/10). Completano il quadro antiriciclaggio 2,5/10, prevenzione 3,0/10 e supporto a vittime e testimoni 1,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Burundi, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Burundi. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Burundi, In Burundi le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Burundi, Il livello governativo di Burundi presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Burundi, Sul piano militare e dual-use, Burundi mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Burundi, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Burundi, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 3,3/10 e il rischio sui dati personali è Alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
0,8	2,4	2,8	4,0	2,3	2,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,5	3,3	3,7	4,9	3,2	3,3

Il GCRI di Burundi è 2,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 3,9/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (4,9/10), mentre il più basso è Supply chain (3,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Alto	Alto	Alto	Alto	Alto	Medio-alto

La matrice applica il FOTR di 3,9/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Burundi, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Burundi, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Burundi, Dal punto di vista italiano, Burundi rientra nella classe «Rischio alto»: cooperazione eccezionale e ad alto controllo, subordinata a assenza di dati sensibili, verifica sanzionatoria, autorizzazioni interne e impossibilità di accesso ai sistemi strategici. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Burundi ricade nella fascia di alto rischio (3,9/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

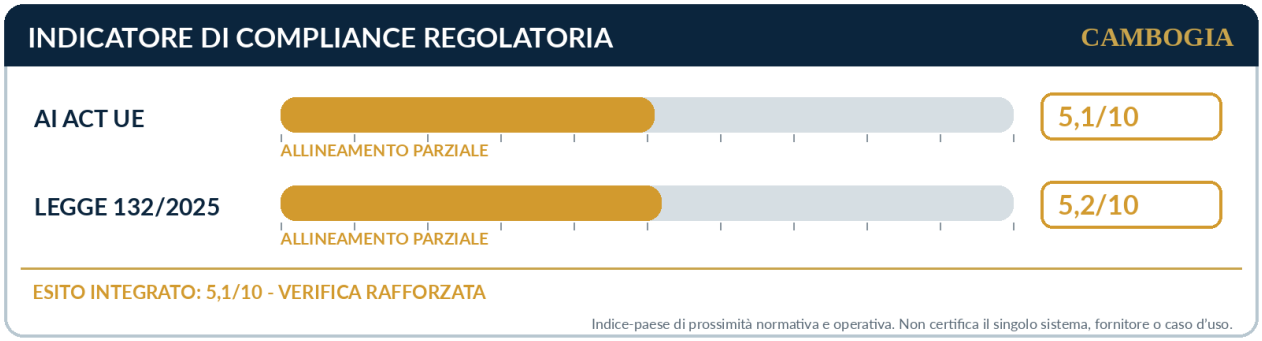
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Burundi: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Cambogia

Posizione FOTR	126	Area	Asia	Subregione	Asia sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,2	GCRI / 10	4,9	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Cambogia, AI Act UE 5,1/10; legge 132/2025 5,2/10; esito integrato 5,1/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Cambogia non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 22/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (4,9/10) e indice FOTR (5,2/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Cambogia è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	68,5% / 4,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	99,2% / 817 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	57,5 / 62,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	37,0/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	34,3/100 - rank 118	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	42/100 - Parzialmente libero / Non libero (22/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,5 / 3,5 / 7,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Cambogia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Cambogia le evidenze principali sono GTMI 62,7/100, EGDI 57,5/100, GCI 37,0/100, AI readiness 34,3/100. La dimensione più robusta è maturità infrastrutturale (6,3/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,1/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Cambogia è 6,3/10. La base statistica rileva utenti Internet pari al 68,5% nel 2024; 4,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 99,2% nel 2024; 817 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Cambogia al posto 118 con un valore medio di 34,3/100; il pilastro migliore è governance (53,4/100), quello più debole è politiche pubbliche (19,5/100). Il GTMI 2025 è 62,7/100. Il punteggio S2 è 4,1/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Cambogia è valutata fragile, con S3 pari a 4,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 51,5/100, sviluppo e diffusione dell'IA 26,2/100, penetrazione Internet 68,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Cambogia ottiene S4 5,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Cambogia, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo

societario e subfornitura. L'impatto sulla valutazione è misurato da S4=5,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Cambogia è S5 4,3/10. La base ITU registra ITU GCI 37,0/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (4,6/20). Freedom on the Net è 42/100 - Parzialmente libero, mentre Freedom in the World è Non libero (22/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,5	Crimini finanziari	8,5
Reti criminali	7,5	Attori incorporati nello Stato	9,0
Attori stranieri	8,0	Attori del settore privato	7,0
Resilienza complessiva	3,5	Cooperazione internazionale	5,0
Politiche e norme nazionali	4,0	Forze dell'ordine	2,5
Antiriciclaggio	4,0	Prevenzione	3,0
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	7,6 - ALTO

Quadro criminale digitale. Per Cambogia, l'indice operativo FOTR-CY è 7,6/10, classe alta. Il mercato dei reati cyber-dipendenti è molto elevato (7,5/10), mentre i crimini finanziari sono molto elevati (8,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e attori stranieri (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Cambogia assumono particolare rilevanza centri organizzati di truffa, frodi d'investimento e sentimentali, phishing multicanale, batterie di schede SIM, conti prestanome, riciclaggio in cripto-attività e compromissione di servizi esternalizzati. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Cambogia, la resilienza complessiva è molto debole (3,5/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono deboli (4,0/10) e la capacità delle forze dell'ordine è molto debole (2,5/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 3,0/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Cambogia, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; controllo della filiera contro esposizione a complessi organizzati per truffe telematiche, call center coercitivi e conti prestanome; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Cambogia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Cambogia, In Cambogia le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Cambogia, Il livello governativo di Cambogia presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Cambogia, Sul piano militare e dual-use, Cambogia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Cambogia, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Cambogia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,9/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,3	4,1	4,5	5,1	4,3	4,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,1	5,7	5,0	5,4	5,2	4,9

Il GCRI di Cambogia è 4,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Maturità cyber (5,7/10), mentre il più basso è Trasferibilità dati (4,9/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 5,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Cambogia, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Cambogia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Cambogia, Dal punto di vista italiano, Cambogia rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Cambogia è indicata una cooperazione selettiva, coerente con il FOTR di 5,2/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

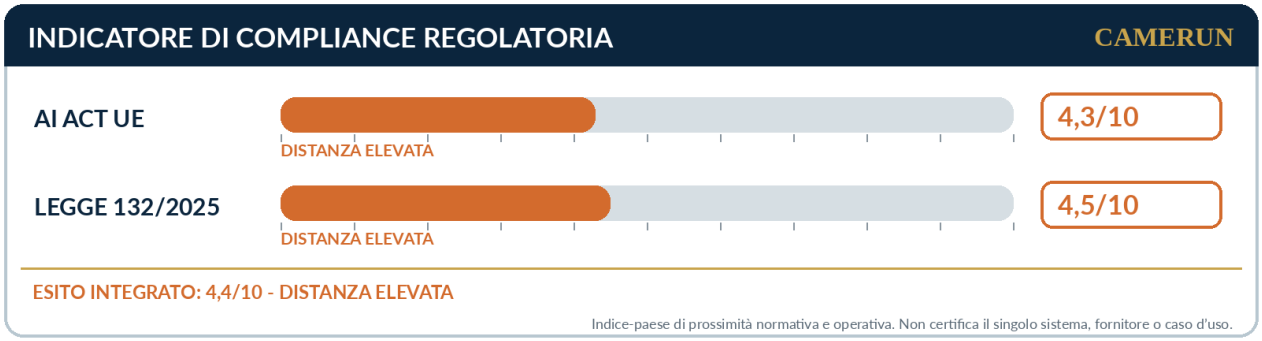
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Cambogia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Camerun

Posizione FOTR	162	Area	Africa	Subregione	Africa centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,4	GCRI / 10	4,4	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Camerun, AI Act UE 4,3/10; legge 132/2025 4,5/10; esito integrato 4,4/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Camerun è stato membro delle nazioni unite collocato in Africa centrale. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 15/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (4,4/10) e indice FOTR (4,4/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per Camerun non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	46,3% / 2,1 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	72,0% / 25 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	42,9 / 37,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	65,5/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	35,8/100 - rank 116	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (15/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 3,1 / 6,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Camerun, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Camerun le evidenze principali sono GTMI 37,8/100, EGDI 42,9/100, GCI 65,5/100, AI readiness 35,8/100. La dimensione più robusta è postura di sicurezza cyber (5,8/10), mentre la criticità relativa riguarda maturità infrastrutturale (3,7/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Camerun è 3,7/10. La base statistica rileva utenti Internet pari al 46,3% nel 2024; 2,1 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 72,0% nel 2024; 25 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Camerun al posto 116 con un valore medio di 35,8/100; il pilastro migliore è governance (53,8/100), quello più debole è adozione pubblica (22,5/100). Il GTMI 2025 è 37,8/100. Il punteggio S2 è 3,7/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Camerun è valutata fragile, con S3 pari a 4,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 51,9/100, sviluppo e diffusione dell'IA 29,2/100, penetrazione Internet 46,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Camerun ottiene S4 4,5/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Camerun, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,5/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Camerun è S5 5,8/10. La base ITU registra ITU GCI 65,5/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (6,2/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (15/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	6,5
Reti criminali	7,5	Attori incorporati nello Stato	8,5
Attori stranieri	7,5	Attori del settore privato	3,5
Resilienza complessiva	3,1	Cooperazione internazionale	5,5
Politiche e norme nazionali	4,5	Forze dell'ordine	3,5
Antiriciclaggio	3,5	Prevenzione	3,0
Supporto vittime e testimoni	2,5	Rischio operativo FOTR-CY	6,5 - ALTO

Pressione del crimine digitale. Il profilo di Camerun restituisce un rischio FOTR-CY di 6,5/10 (alto). La componente cyber-dipendente vale 5,0/10 e quella finanziaria 6,5/10; la risposta sistemica è valutata molto debole, con resilienza media di 3,1/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,5/10) e reti criminali (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Camerun assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Camerun, la resilienza complessiva è molto debole (3,1/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono deboli (4,5/10) e la capacità delle forze dell'ordine è debole (3,5/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 3,0/10 e supporto a vittime e testimoni 2,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Camerun, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Camerun. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Camerun, In Camerun le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Camerun, Il livello governativo di Camerun presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Camerun, Sul piano militare e dual-use, Camerun mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Camerun, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Camerun, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,1/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,7	3,7	4,5	4,5	5,8	4,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,5	4,6	4,1	5,1	4,3	4,1

Il GCRI di Camerun è 4,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,1/10), mentre il più basso è Trasparenza istituzionale (4,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Camerun, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Camerun, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Camerun, Dal punto di vista italiano, Camerun rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Camerun ricade nella fascia di alto rischio (4,4/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

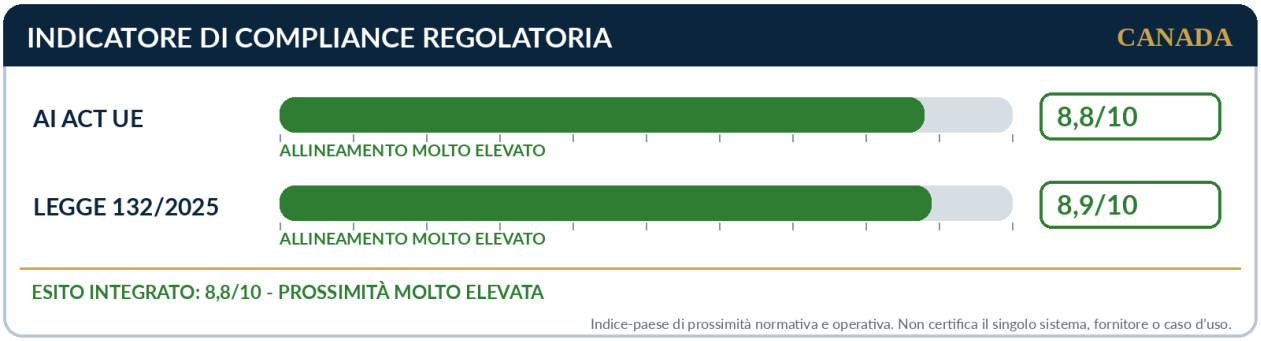
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Camerun: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Canada

Posizione FOTR	10	Area	Americhe	Subregione	Nord America e Artico
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	9,0	GCRI / 10	8,1	Classe operativa	Affidabilità molto alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Canada, AI Act UE 8,8/10; legge 132/2025 8,9/10; esito integrato 8,8/10, classe «Allineamento molto elevato». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Nel quadro di Americhe, Canada presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La partecipazione all'ecosistema Five Eyes rafforza l'integrazione informativa e tecnologica con il blocco anglosassone, ma rende necessario valutare i poteri di accesso extraterritoriale e la concentrazione cloud. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 97/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,1/10) e indice FOTR (9,0/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per un operatore italiano, Canada costituisce un ambiente digitale ad alta affidabilità: connettività, supervisione e continuità sono solide. La valutazione non deve però trascurare subfornitori, accessi transfrontalieri e tecnologie dual-use.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	94,4% / 42,5 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 39.738 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	84,5 / 94,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	93,2/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	76,1/100 - rank 12	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	85/100 - Libero / Libero (97/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,0 / 7,4 / 4,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Canada, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Canada le evidenze principali sono GTMI 94,9/100, EGDI 84,5/100, GCI 93,2/100, AI readiness 76,1/100. La dimensione più robusta è maturità infrastrutturale (9,1/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,6/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Canada è 9,1/10. La base statistica rileva utenti Internet pari al 94,4% nel 2024; 42,5 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 39.738 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Canada al posto 12 con un valore medio di 76,1/100; il pilastro migliore è politiche pubbliche (92,5/100), quello più debole è resilienza (67,6/100). Il GTMI 2025 è 94,9/100. Il punteggio S2 è 8,1/10 e indica una capacità elevata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Canada è valutata sufficiente ma disomogenea, con S3 pari a 7,9/10. Le evidenze disponibili comprendono indice UN di capitale umano 87,2/100, sviluppo e diffusione dell'IA 69,0/100, penetrazione Internet 94,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Canada ottiene S4 6,6/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Canada, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=6,6/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Canada è S5 9,0/10. La base ITU registra ITU GCI 93,2/100, Tier 2 - avanzato; il pilastro relativamente più debole è misure tecniche (15,3/20). Freedom on the Net è 85/100 - Libero, mentre Freedom in the World è Libero (97/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: PIPEDA e leggi provinciali; discipline settoriali e di sicurezza critica. L'adeguatezza UE riguarda le organizzazioni commerciali comprese nell'ambito riconosciuto.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,0	Crimini finanziari	5,0
Reti criminali	5,0	Attori incorporati nello Stato	2,0
Attori stranieri	4,5	Attori del settore privato	4,5
Resilienza complessiva	7,4	Cooperazione internazionale	8,5
Politiche e norme nazionali	8,0	Forze dell'ordine	7,5
Antiriciclaggio	6,0	Prevenzione	6,5
Supporto vittime e testimoni	8,5	Rischio operativo FOTR-CY	4,7 - MODERATO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (7,0/10), criminalità finanziaria (5,0/10) e resilienza (7,4/10) colloca Canada in una fascia di rischio moderato, pari a 4,7/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (5,0/10) e attori stranieri (4,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Canada assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, compromissione della supply chain, compromissione delle caselle di posta aziendale, furto d'identità, abuso di servizi cloud e riciclaggio digitale; l'elevata capacità di denuncia aumenta la visibilità statistica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Canada, la resilienza complessiva è intermedia (7,4/10); la cooperazione internazionale è robusta (8,5/10), le politiche e norme nazionali sono robuste (8,0/10) e la capacità delle forze dell'ordine è robusta (7,5/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 6,5/10 e supporto a vittime e testimoni 8,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Canada, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Canada. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Canada, In Canada le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Canada, Il livello governativo di Canada presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Canada, Sul piano militare e dual-use, Canada mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Canada, PIPEDA e leggi provinciali; discipline settoriali e di sicurezza critica. L'adeguatezza UE riguarda le organizzazioni commerciali comprese nell'ambito riconosciuto. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Canada, È disponibile una decisione UE di adeguatezza entro l'ambito commerciale riconosciuto. L'operatore italiano deve comunque controllare la portata della decisione, i trasferimenti successivi, le misure di sicurezza e le eventuali discipline settoriali. La componente FOTR di trasferibilità è 10,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,1	8,1	7,9	6,6	9,0	8,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,6	10,0	7,0	10,0	8,6	10,0

Il GCRI di Canada è 8,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 9,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Maturità cyber (10,0/10), mentre il più basso è Trasparenza istituzionale (7,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Basso	Medio-basso	Basso	Basso

La matrice applica il FOTR di 9,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Canada, la cautela si concentra su 2 ambiti a rischio intermedio: Sanità e biometria, IP e R&S. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Canada, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Canada, Dal punto di vista italiano, Canada rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Canada, il FOTR di 9,0/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (7,0/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

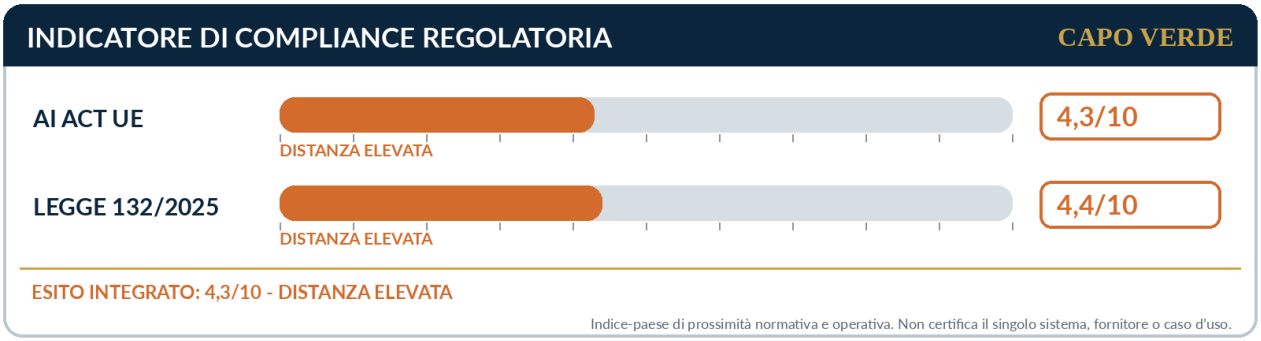
Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Canada: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Capo Verde

Posizione FOTR	171	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,3	GCRI / 10	4,8	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Capo Verde, AI Act UE 4,3/10; legge 132/2025 4,4/10; esito integrato 4,3/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Capo Verde, situato in Africa occidentale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 92/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (4,8/10) e indice FOTR (4,3/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per Capo Verde non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	74,7% / 8,3 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	98,4% / 857 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	62,4 / 77,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	51,5/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	33,5/100 - rank 122	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (92/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,5 / 6,5 / 4,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Capo Verde, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Capo Verde le evidenze principali sono GTMI 77,4/100, EGDI 62,4/100, GCI 51,5/100, AI readiness 33,5/100. La dimensione più robusta è maturità infrastrutturale (6,1/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (4,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Capo Verde è 6,1/10. La base statistica rileva utenti Internet pari al 74,7% nel 2024; 8,3 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 98,4% nel 2024; 857 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Capo Verde al posto 122 con un valore medio di 33,5/100; il pilastro migliore è adozione pubblica (66,5/100), quello più debole è sviluppo e diffusione (11,6/100). Il GTMI 2025 è 77,4/100. Il punteggio S2 è 4,7/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Capo Verde è valutata fragile, con S3 pari a 4,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 56,9/100, sviluppo e diffusione dell'IA 11,6/100, penetrazione Internet 74,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Capo Verde ottiene S4 4,3/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Capo Verde, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre

ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,3/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Capo Verde è S5 4,8/10. La base ITU registra ITU GCI 51,5/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è sviluppo delle capacità (2,2/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (92/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,5	Crimini finanziari	4,0
Reti criminali	5,0	Attori incorporati nello Stato	4,0
Attori stranieri	6,5	Attori del settore privato	4,5
Resilienza complessiva	6,5	Cooperazione internazionale	8,0
Politiche e norme nazionali	7,0	Forze dell'ordine	6,0
Antiriciclaggio	5,5	Prevenzione	6,5
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	4,1 - MODERATO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (3,5/10), criminalità finanziaria (4,0/10) e resilienza (6,5/10) colloca Capo Verde in una fascia di rischio moderato, pari a 4,1/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (6,5/10) e reti criminali (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Capo Verde assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Capo Verde, la resilienza complessiva è intermedia (6,5/10); la cooperazione internazionale è robusta (8,0/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è intermedia (6,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 6,5/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Capo Verde, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Capo Verde. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Capo Verde, In Capo Verde le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Capo Verde, Il livello governativo di Capo Verde presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Capo Verde, Sul piano militare e dual-use, Capo Verde mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Capo Verde, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Capo Verde, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,1/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,1	4,7	4,1	4,3	4,8	4,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,4	3,9	4,5	4,8	3,9	4,1

Il GCRI di Capo Verde è 4,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,3/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (4,8/10), mentre il più basso è Maturità cyber (3,9/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,3/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Capo Verde, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Capo Verde, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Capo Verde, Dal punto di vista italiano, Capo Verde rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Capo Verde ricade nella fascia di alto rischio (4,3/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

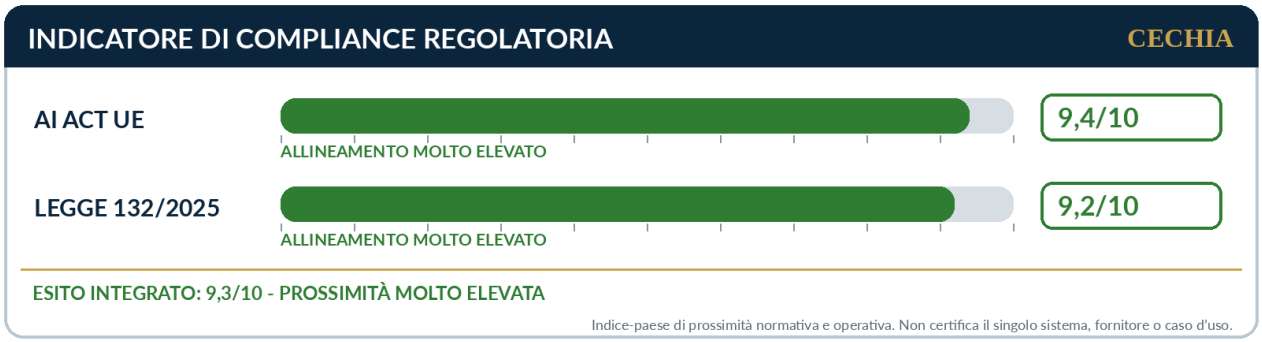
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Capo Verde: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Cechia

Posizione FOTR	25	**Area**	Europa	**Subregione**	Europa occidentale e centrale
Status	Stato membro delle Nazioni Unite	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	8,5	**GCRI / 10**	7,7	**Classe operativa**	**Affidabilità alta**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Cechia, AI Act UE 9,4/10; legge 132/2025 9,2/10; esito integrato 9,3/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Per un operatore italiano, Cechia non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 95/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,7/10) e indice FOTR (8,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Cechia presenta un ecosistema digitale maturo, istituzioni generalmente prevedibili e una buona capacità di gestione degli incidenti. Il rischio residuo deriva soprattutto dalla concentrazione cloud, dalle dipendenze extraeuropee e dalla complessità delle filiere software.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	87,7% / 38,9 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 79.336 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	82,4 / 86,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	87,9/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	67,5/100 - rank 32	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (95/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 6,5 / 4,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Cechia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Cechia le evidenze principali sono GTMI 86,3/100, EGDI 82,4/100, GCI 87,9/100, AI readiness 67,5/100. La dimensione più robusta è maturità infrastrutturale (9,4/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,2/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Cechia è 9,4/10. La base statistica rileva utenti Internet pari al 87,7% nel 2024; 38,9 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 79.336 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Cechia al posto 32 con un valore medio di 67,5/100; il pilastro migliore è politiche pubbliche (81,0/100), quello più debole è sviluppo e diffusione (54,0/100). Il GTMI 2025 è 86,3/100. Il punteggio S2 è 7,1/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Cechia è valutata sufficiente ma disomogenea, con S3 pari a 7,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 85,1/100, sviluppo e diffusione dell'IA 54,0/100, penetrazione Internet 87,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Cechia ottiene S4 6,2/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open

source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Cechia, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario, luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,2/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Cechia è S5 8,5/10. La base ITU registra ITU GCI 87,9/100, Tier 2 - avanzato; il pilastro relativamente più debole è cooperazione (14,3/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (95/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, legge nazionale sul trattamento dei dati personali e quadro cyber aggiornato alla direttiva NIS2.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	6,0
Reti criminali	4,5	Attori incorporati nello Stato	4,5
Attori stranieri	5,0	Attori del settore privato	5,0
Resilienza complessiva	6,5	Cooperazione internazionale	7,0
Politiche e norme nazionali	7,0	Forze dell'ordine	7,0
Antiriciclaggio	6,5	Prevenzione	6,0
Supporto vittime e testimoni	5,5	Rischio operativo FOTR-CY	4,8 - MODERATO

Quadro criminale digitale. Per Cechia, l'indice operativo FOTR-CY è 4,8/10, classe moderata. Il mercato dei reati cyber-dipendenti è elevato (5,5/10), mentre i crimini finanziari sono elevati (6,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (5,0/10) e attori del settore privato (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Cechia assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Cechia, la resilienza complessiva è intermedia (6,5/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è intermedia (7,0/10). Completano il quadro antiriciclaggio 6,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 5,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Cechia, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Cechia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Cechia, In Cechia le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La disponibilità

del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Cechia, Il livello governativo di Cechia presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Cechia, Sul piano militare e dual-use, Cechia mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Cechia, GDPR, legge nazionale sul trattamento dei dati personali e quadro cyber aggiornato alla direttiva NIS2. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Cechia, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,3/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,4	7,1	7,5	6,2	8,5	7,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,1	8,1	7,9	9,1	7,6	9,3

Il GCRI di Cechia è 7,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,3/10), mentre il più basso è Supply chain (7,6/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Cechia, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Cechia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Cechia, Dal punto di vista italiano, Cechia rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Cechia, il FOTR di 8,5/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (7,6/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

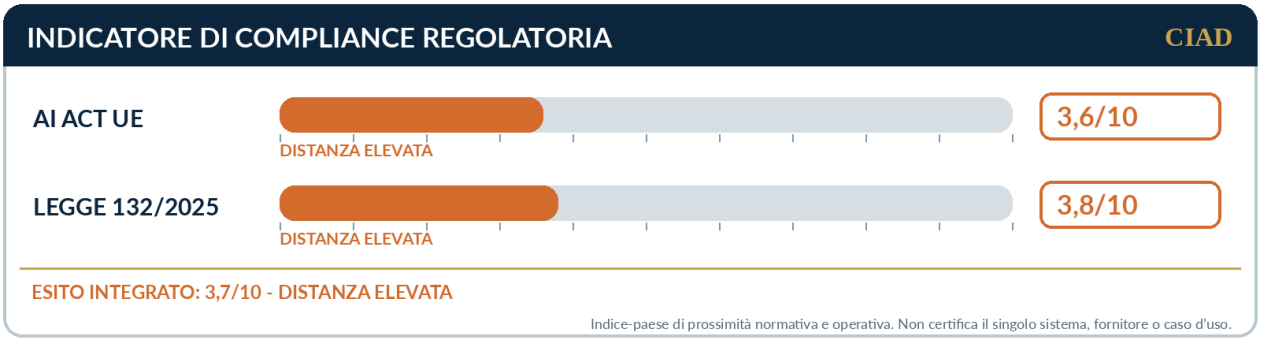
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Cechia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Ciad

Posizione FOTR	178	Area	Africa	Subregione	Africa centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	3,8	GCRI / 10	2,6	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Ciad, AI Act UE 3,6/10; legge 132/2025 3,8/10; esito integrato 3,7/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Ciad è stato membro delle nazioni unite collocato in Africa centrale. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 15/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (3,8/10) supera il GCRI tecnico (2,6/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Ciad presenta un livello di rischio elevato per cooperazione digitale, dovuto a limitata trasparenza, poteri pubblici, instabilità o dipendenze tecnologiche. Le attività dovrebbero escludere dati sensibili e asset strategici.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	12,6% / 0,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	13,4% / 1 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	17,9 / 10,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	48,7/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	18,4/100 - rank 182	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (15/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,5 / 2,3 / 5,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Ciad, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Ciad le evidenze principali sono GTMI 10,6/100, EGDI 17,9/100, GCI 48,7/100, AI readiness 18,4/100. La dimensione più robusta è postura di sicurezza cyber (4,3/10), mentre la criticità relativa riguarda maturità infrastrutturale (1,0/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Ciad è 1,0/10. La base statistica rileva utenti Internet pari al 12,6% nel 2024; 0,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 13,4% nel 2024; 1 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Ciad al posto 182 con un valore medio di 18,4/100; il pilastro migliore è governance (48,7/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 10,6/100. Il punteggio S2 è 1,8/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Ciad è valutata fragile, con S3 pari a 2,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 14,9/100, sviluppo e diffusione dell'IA 10,1/100, penetrazione Internet 12,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Ciad ottiene S4 3,9/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Ciad, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=3,9/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Ciad è S5 4,3/10. La base ITU registra ITU GCI 48,7/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (3,2/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (15/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,5	Crimini finanziari	4,5
Reti criminali	7,0	Attori incorporati nello Stato	8,5
Attori stranieri	6,5	Attori del settore privato	6,0
Resilienza complessiva	2,3	Cooperazione internazionale	4,5
Politiche e norme nazionali	3,0	Forze dell'ordine	2,5
Antiriciclaggio	1,5	Prevenzione	1,5
Supporto vittime e testimoni	1,5	Rischio operativo FOTR-CY	5,7 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Ciad restituisce un rischio FOTR-CY di 5,7/10 (significativo). La componente cyber-dipendente vale 2,5/10 e quella finanziaria 4,5/10; la risposta sistemica è valutata molto debole, con resilienza media di 2,3/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,5/10) e reti criminali (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Ciad assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Ciad, la resilienza complessiva è molto debole (2,3/10); la cooperazione internazionale è debole (4,5/10), le politiche e norme nazionali sono molto deboli (3,0/10) e la capacità delle forze dell'ordine è molto debole (2,5/10). Completano il quadro antiriciclaggio 1,5/10, prevenzione 1,5/10 e supporto a vittime e testimoni 1,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Ciad, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Ciad. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Ciad, In Ciad le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. Per i

partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Ciad, Il livello governativo di Ciad presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Ciad, Sul piano militare e dual-use, Ciad mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Ciad, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Ciad, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 3,3/10 e il rischio sui dati personali è Alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
1,0	1,8	2,2	3,9	4,3	2,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,3	3,4	3,3	4,9	3,4	3,3

Il GCRI di Ciad è 2,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 3,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (4,9/10), mentre il più basso è Trasparenza istituzionale (3,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Alto	Alto	Alto	Alto	Alto	Alto

La matrice applica il FOTR di 3,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Ciad, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Ciad, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Ciad, Dal punto di vista italiano, Ciad rientra nella classe «Rischio alto»: cooperazione eccezionale e ad alto controllo, subordinata a assenza di dati sensibili, verifica sanzionatoria, autorizzazioni interne e impossibilità di accesso ai sistemi strategici. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Ciad ricade nella fascia di alto rischio (3,8/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

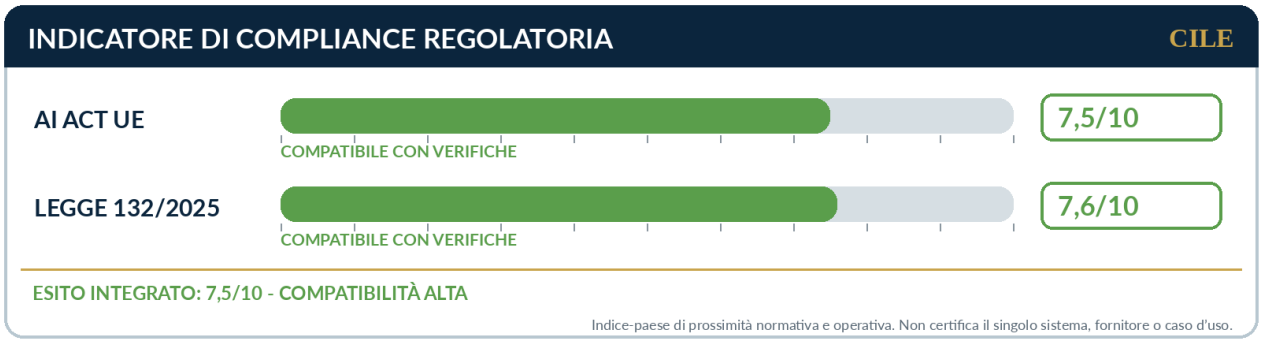
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Ciad: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Cile

Posizione FOTR	46	Area	Americhe	Subregione	America meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	7,5	GCRI / 10	7,3	Classe operativa	Affidabilità favorevole ma condizionata

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Cile, AI Act UE 7,5/10; legge 132/2025 7,6/10; esito integrato 7,5/10, classe «Compatibile con verifiche». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Prima dell'ingaggio occorre una analisi degli scostamenti mirata su trasparenza, governance dei dati, rappresentanza nell'UE, audit e rimedi contrattuali.

Premessa geopolitica e tecnologica

Nel quadro di Americhe, Cile presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 95/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,3/10) e indice FOTR (7,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ambiente digitale di Cile è complessivamente affidabile e aperto agli scambi. Per investimenti italiani è opportuno verificare la disciplina locale, la struttura dei fornitori e gli eventuali poteri pubblici di accesso.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	95,6% / 23,7 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	99,0% / 11.913 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	88,3 / 87,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	70,2/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	62,7/100 - rank 50	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	87/100 - Libero / Libero (95/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 6,2 / 5,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Cile, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Cile le evidenze principali sono GTMI 87,2/100, EGDI 88,3/100, GCI 70,2/100, AI readiness 62,7/100. La dimensione più robusta è maturità infrastrutturale (8,7/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,2/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Cile è 8,7/10. La base statistica rileva utenti Internet pari al 95,6% nel 2024; 23,7 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 99,0% nel 2024; 11.913 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Cile al posto 50 con un valore medio di 62,7/100; il pilastro migliore è politiche pubbliche (92,5/100), quello più debole è sviluppo e diffusione (45,3/100). Il GTMI 2025 è 87,2/100. Il punteggio S2 è 7,0/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Cile è valutata sufficiente ma disomogenea, con S3 pari a 6,9/10. Le evidenze disponibili comprendono indice UN di capitale umano 84,1/100, sviluppo e diffusione dell'IA 45,3/100, penetrazione Internet 95,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Cile ottiene S4 6,2/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Cile, Mercato aperto con fornitori statunitensi, europei e cinesi; buona diversificazione. L'impatto sulla valutazione è misurato da S4=6,2/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Cile è S5 7,5/10. La base ITU registra ITU GCI 70,2/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (11,5/20). Freedom on the Net è 87/100 - Libero, mentre Freedom in the World è Libero (95/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge 19.628 e riforme di rafforzamento della protezione dei dati; architettura cyber in consolidamento e trasferimenti soggetti a garanzie.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	5,0
Reti criminali	6,0	Attori incorporati nello Stato	5,5
Attori stranieri	6,5	Attori del settore privato	5,0
Resilienza complessiva	6,2	Cooperazione internazionale	8,0
Politiche e norme nazionali	6,5	Forze dell'ordine	4,5
Antiriciclaggio	6,5	Prevenzione	6,5
Supporto vittime e testimoni	6,0	Rischio operativo FOTR-CY	5,2 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Cile il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,2/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 5,5/10; le frodi e i reati finanziari 5,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (6,5/10) e reti criminali (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Cile assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Cile, la resilienza complessiva è intermedia (6,2/10); la cooperazione internazionale è robusta (8,0/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 6,5/10, prevenzione 6,5/10 e supporto a vittime e testimoni 6,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Cile, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Cile. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Cile, In Cile le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Cile, Il livello governativo di Cile presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Cile, Sul piano militare e dual-use, Cile mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Cile, Legge 19.628 e riforme di rafforzamento della protezione dei dati; architettura cyber in consolidamento e trasferimenti soggetti a garanzie. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Cile, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 7,4/10 e il rischio sui dati personali è Medio-basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,7	7,0	6,9	6,2	7,5	7,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
7,7	7,3	7,4	8,0	7,4	7,4

Il GCRI di Cile è 7,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 7,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (8,0/10), mentre il più basso è Maturità cyber (7,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 7,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Cile, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Cile, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Cile, Dal punto di vista italiano, Cile rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Cile è favorevole ma condizionata: il valore FOTR di 7,5/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Maturità cyber.

Presidi minimi raccomandati

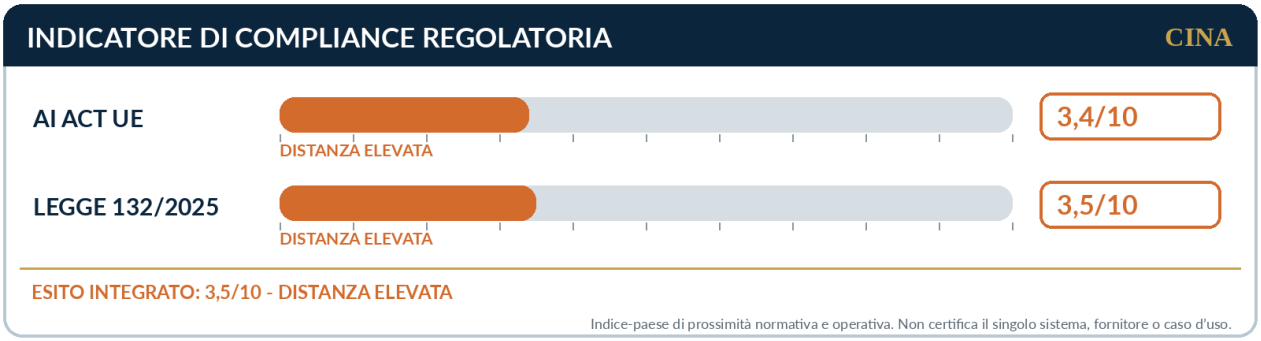
- Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
- Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
- Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
- Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Cile: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Cina

Posizione FOTR	185	Area	Asia	Subregione	Asia orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	3,2	GCRI / 10	7,4	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Cina, AI Act UE 3,4/10; legge 132/2025 3,5/10; esito integrato 3,5/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

La Cina è contemporaneamente una potenza tecnologica sistemica, un grande fornitore di hardware, telecomunicazioni, piattaforme, energia digitale e intelligenza artificiale, e un ordinamento caratterizzato da forte direzione statale dei dati e delle infrastrutture. La capacità tecnica del Paese è quindi molto superiore al livello di affidabilità attribuibile, dal punto di vista italiano, alla condivisione di informazioni sensibili o all'accesso continuativo a reti strategiche. Il divario tra GCRI tecnico e indice FOTR è intenzionale: segnala che potenza industriale, maturità cyber e capacità di produzione non coincidono con compatibilità giuridica, trasparenza, reciprocità o assenza di interferenze pubbliche. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 9/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (7,4/10) è superiore al punteggio FOTR (3,2/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Ecosistema digitale di scala globale, fortemente integrato con indirizzo statale, localizzazione, controlli sui dati e politiche industriali; la cooperazione richiede separazione tecnica e governance molto restrittiva.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	91,6% / 47,2 per 100	2025/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 1.413 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	87,2 / 65,1	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	91,6/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	77,2/100 - rank 8	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	9/100 - Non libero / Non libero (9/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	8,5 / 5,5 / 6,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Cina, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Cina le evidenze principali sono GTMI 65,1/100, EGDI 87,2/100, GCI 91,6/100, AI readiness 77,2/100. La dimensione più robusta è maturità infrastrutturale (9,0/10), mentre la criticità relativa riguarda postura di sicurezza cyber (5,9/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Cina è 9,0/10. La base statistica rileva utenti Internet pari al 91,6% nel 2025; 47,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 1.413 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Cina al posto 8 con un valore medio di 77,2/100; il pilastro migliore è politiche pubbliche (92,5/100), quello più debole è adozione pubblica (49,0/100). Il GTMI 2025 è 65,1/100. Il punteggio S2 è 7,7/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Cina è valutata sufficiente ma disomogenea, con S3 pari a 7,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 79,0/100, sviluppo e diffusione dell'IA 74,7/100, penetrazione Internet 91,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Cina ottiene S4 7,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 8,8/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Cina, Fornitura prevalentemente domestica, sostenuta da grandi gruppi cinesi; dipendenze estere residue in componenti avanzati e strumenti di produzione dei semiconduttori. L'impatto sulla valutazione è

misurato da S4=7,3/10 e dal proxy di indipendenza 8,8/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Cina è S5 5,9/10. La base ITU registra ITU GCI 91,6/100, Tier 2 - avanzato; il pilastro relativamente più debole è misure tecniche (17,1/20). Freedom on the Net è 9/100 - Non libero, mentre Freedom in the World è Non libero (9/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Cybersecurity Law, Data Security Law, Personal Information Protection Law, MLPS e regole CAC sui trasferimenti e sulla sicurezza nazionale; localizzazione e accessi pubblici richiedono valutazioni molto restrittive.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	8,5	Crimini finanziari	7,5
Reti criminali	7,5	Attori incorporati nello Stato	7,0
Attori stranieri	2,0	Attori del settore privato	7,0
Resilienza complessiva	5,5	Cooperazione internazionale	6,5
Politiche e norme nazionali	7,0	Forze dell'ordine	6,0
Antiriciclaggio	6,5	Prevenzione	5,5
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	6,6 - ALTO

Rischio criminale connesso alle tecnologie. In Cina il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 6,6/10, livello alto. I reati che dipendono direttamente da sistemi informatici raggiungono 8,5/10; le frodi e i reati finanziari 7,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (7,5/10) e attori incorporati nello Stato (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Cina assumono particolare rilevanza compromissioni della supply chain, sottrazione di proprietà intellettuale, furto di cripto-attività, phishing mirato, abuso di identità digitali e intrusioni persistenti contro industria e amministrazioni. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Cina, la resilienza complessiva è intermedia (5,5/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è intermedia (6,0/10). Completano il quadro antiriciclaggio 6,5/10, prevenzione 5,5/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Cina, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Cina. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Cina, In Cina le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Cina, Il livello governativo di Cina presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Cina, Sul piano militare e dual-use, Cina mostra forte ruolo statale e integrazione con filiere cinesi o nazionali, con limitata trasparenza esterna. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Cina, Cybersecurity Law, Data Security Law, Personal Information Protection Law, MLPS e regole CAC sui trasferimenti e sulla sicurezza nazionale; localizzazione e accessi pubblici richiedono valutazioni molto restrittive. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Cina, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 1,6/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,0	7,7	7,1	7,3	5,9	7,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
2,8	5,1	1,9	3,5	4,4	1,6

Il GCRI di Cina è 7,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 3,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (5,1/10), mentre il più basso è Trasferibilità dati (1,6/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Alto	Medio-alto	Alto	Alto	Alto

La matrice applica il FOTR di 3,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Cina, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Cina, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Cina, Dal punto di vista italiano, Cina rientra nella classe «Rischio alto»: cooperazione eccezionale e ad alto controllo, subordinata a assenza di dati sensibili, verifica sanzionatoria, autorizzazioni interne e impossibilità di accesso ai sistemi strategici. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Cina, il FOTR di 3,2/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

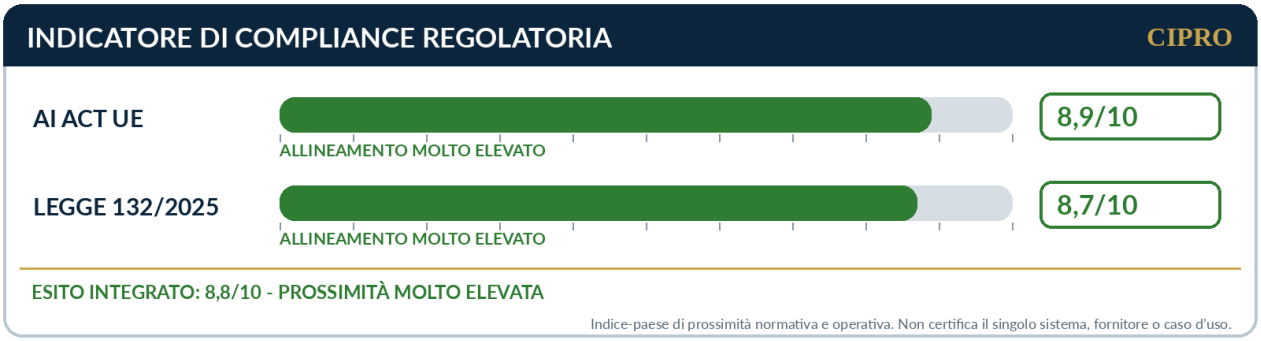
Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.
Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.
Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Cina: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Cipro

Posizione FOTR	34	Area	Europa	Subregione	Europa sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,1	GCRI / 10	7,7	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Cipro, AI Act UE 8,9/10; legge 132/2025 8,7/10; esito integrato 8,8/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Per un operatore italiano, Cipro non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. L'appartenenza all'Unione europea inserisce il Paese nel mercato digitale unico, nel sistema GDPR e nelle principali discipline comuni su cybersicurezza, dati e intelligenza artificiale. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 90/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,7/10) e indice FOTR (8,1/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Cipro offre condizioni favorevoli alla cooperazione tecnologica, con capacità istituzionali e cyber generalmente robuste. Restano differenze settoriali che rendono necessaria una verifica preventiva proporzionata ai dati e alla criticità del progetto.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	89,6% / 37,6 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 221.298 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	86,2 / 79,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	98,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	62,8/100 - rank 47	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (90/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 4,5 / 5,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Cipro, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Cipro le evidenze principali sono GTMI 79,0/100, EGDI 86,2/100, GCI 98,0/100, AI readiness 62,8/100. La dimensione più robusta è maturità infrastrutturale (9,3/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Cipro è 9,3/10. La base statistica rileva utenti Internet pari al 89,6% nel 2024; 37,6 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 221.298 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Cipro al posto 47 con un valore medio di 62,8/100; il pilastro migliore è adozione pubblica (81,3/100), quello più debole è sviluppo e diffusione (36,1/100). Il GTMI 2025 è 79,0/100. Il punteggio S2 è 6,8/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Cipro è valutata sufficiente ma disomogenea, con S3 pari a 7,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 87,0/100, sviluppo e diffusione dell'IA 36,1/100, penetrazione Internet 89,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Cipro ottiene S4 6,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Cipro, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Cipro è S5 9,0/10. La base ITU registra ITU GCI 98,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è sviluppo delle capacità (18,6/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (90/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR e normativa nazionale sulla protezione dei dati e sulla sicurezza delle reti; applicazione del corpus digitale UE.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	5,5
Reti criminali	5,0	Attori incorporati nello Stato	4,0
Attori stranieri	7,0	Attori del settore privato	5,0
Resilienza complessiva	4,5	Cooperazione internazionale	7,0
Politiche e norme nazionali	6,0	Forze dell'ordine	5,5
Antiriciclaggio	3,5	Prevenzione	4,0
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	5,2 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (4,5/10), criminalità finanziaria (5,5/10) e resilienza (4,5/10) colloca Cipro in una fascia di rischio significativo, pari a 5,2/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (7,0/10) e reti criminali (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Cipro assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Cipro, la resilienza complessiva è debole (4,5/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 4,0/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Cipro, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Cipro. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Cipro, In Cipro le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Cipro, Il livello governativo di Cipro presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Cipro, Sul piano militare e dual-use, Cipro mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Cipro, GDPR e normativa nazionale sulla protezione dei dati e sulla sicurezza delle reti; applicazione del corpus digitale UE. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Cipro, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,3	6,8	7,2	6,1	9,0	7,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,5	7,3	7,8	8,6	7,4	9,0

Il GCRI di Cipro è 7,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,1/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,0/10), mentre il più basso è Maturità cyber (7,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,1/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Cipro, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Cipro, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Cipro, Dal punto di vista italiano, Cipro rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Cipro, il FOTR di 8,1/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Maturità cyber (7,3/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

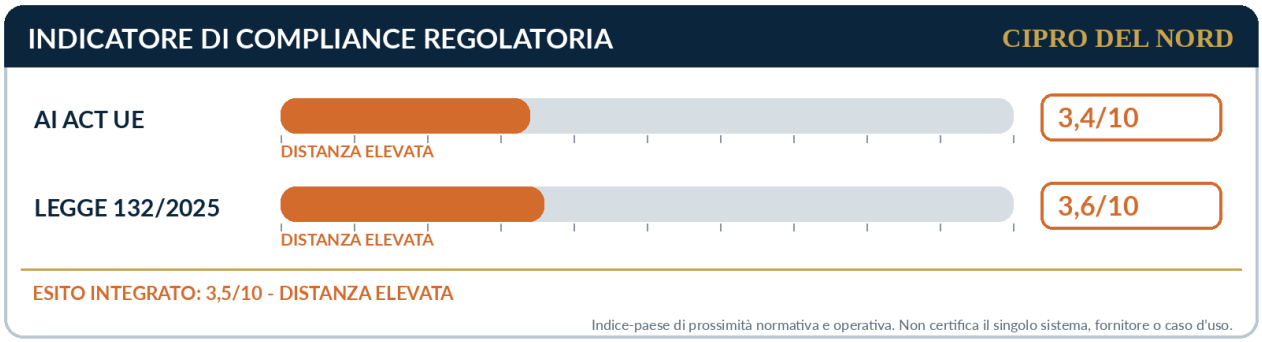
Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Cipro: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Cipro del Nord

Posizione FOTR	184	Area	Europa	Subregione	Mediterraneo orientale
Status	Entità de facto riconosciuta dalla sola Turchia	Confidenza Celeborn Intelligence	Bassa	Copertura dati	0/7 famiglie
FOTR / 10	3,4	GCRI / 10	2,9	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Cipro del Nord, AI Act UE 3,4/10; legge 132/2025 3,6/10; esito integrato 3,5/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Cipro del Nord è entità de facto riconosciuta dalla sola turchia collocato in Mediterraneo orientale. La prossimità europea può ridurre i costi operativi, ma non sostituisce la verifica dell'allineamento al GDPR, delle autorità indipendenti e della reale origine dei servizi cloud. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Turchia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 75/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (2,9/10) e indice FOTR (3,4/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Ecosistema dipendente dalla Turchia e privo di riconoscimento generale; validità contrattuale, trasferimenti e rimedi richiedono una verifica specialistica.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	n.d. / n.d. per 100	n.d./n.d.	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	n.d. / n.d. per milione	n.d./n.d.	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	n.d. / n.d.	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	n.d./100 - n.d.	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	n.d./100 - rank n.d.	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (75/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,1 / 4,2 / 6,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Cipro del Nord, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 0/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Cipro del Nord le evidenze principali sono nessun indicatore composito pienamente comparabile. La dimensione più robusta è maturità infrastrutturale (3,9/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (1,8/10). Sono disponibili 0 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata bassa. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Cipro del Nord è 3,9/10. La base statistica rileva i principali dati WDI non sono disponibili in forma omogenea. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Per Cipro del Nord non è disponibile un profilo Oxford Insights direttamente attribuibile; l'adozione di IA è quindi valutata attraverso GovTech, servizi online, infrastrutture e fonti qualitative. Il punteggio S2 è 3,7/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Cipro del Nord è valutata fragile, con S3 pari a 1,8/10. Le evidenze disponibili comprendono evidenza quantitativa incompleta. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Cipro del Nord ottiene S4 3,0/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Turchia; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Cipro del Nord, Dipendenza predominante dalla Turchia per connettività, piattaforme e servizi pubblici. L'impatto sulla valutazione è misurato da S4=3,0/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Cipro del Nord è S5 2,2/10. La base ITU registra GCI non disponibile in forma comparabile. Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (75/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Disciplina nazionale della protezione dei dati, delle comunicazioni elettroniche e dei reati informatici, con differenze rispetto al GDPR; trasferimenti e accessi pubblici richiedono una verifica locale aggiornata.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,1	Crimini finanziari	7,2
Reti criminali	6,7	Attori incorporati nello Stato	6,8
Attori stranieri	6,7	Attori del settore privato	5,6
Resilienza complessiva	4,2	Cooperazione internazionale	5,9
Politiche e norme nazionali	5,5	Forze dell'ordine	4,4
Antiriciclaggio	3,2	Prevenzione	3,7
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	6,4 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (5,1/10), criminalità finanziaria (7,2/10) e resilienza (4,2/10) colloca Cipro del Nord in una fascia di rischio significativo, pari a 6,4/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (6,8/10) e attori stranieri (6,7/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Cipro del Nord assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Cipro del Nord, la resilienza complessiva è debole (4,2/10); la cooperazione internazionale è intermedia (5,9/10), le politiche e norme nazionali sono deboli (5,5/10) e la capacità delle forze dell'ordine è debole (4,4/10). Completano il quadro antiriciclaggio 3,2/10, prevenzione 3,7/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Cipro del Nord, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative. Poiché l'entità non dispone di una serie nazionale GI-TOC autonoma, i valori derivano da un proxy Celeborn Intelligence ponderato su Cipro 45%, Turchia 55%; la confidenza deve pertanto essere considerata inferiore e la decisione resa più prudente.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; proxy Celeborn Intelligence ponderato su Cipro 45%, Turchia 55%. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Cipro del Nord, In Cipro del Nord le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Cipro del Nord, Il livello governativo di Cipro del Nord presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Cipro del Nord, Sul piano militare e dual-use, Cipro del Nord mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Cipro del Nord, Disciplina nazionale della protezione dei dati, delle comunicazioni elettroniche e dei reati informatici, con differenze rispetto al GDPR; trasferimenti e accessi pubblici richiedono una verifica locale aggiornata. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Cipro del Nord, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 2,0/10 e il rischio sui dati personali è Alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,9	3,7	1,8	3,0	2,2	2,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,0	4,3	1,8	4,1	4,4	2,0

Il GCRI di Cipro del Nord è 2,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 3,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Supply chain (4,4/10), mentre il più basso è Trasparenza istituzionale (1,8/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Alto	Alto	Medio-alto	Alto	Alto	Alto

La matrice applica il FOTR di 3,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Cipro del Nord, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Cipro del Nord, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Cipro del Nord, Dal punto di vista italiano, Cipro del Nord rientra nella classe «Rischio alto»: cooperazione eccezionale e ad alto controllo, subordinata a assenza di dati sensibili, verifica sanzionatoria, autorizzazioni interne e impossibilità di accesso ai sistemi strategici. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Cipro del Nord, il FOTR di 3,4/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

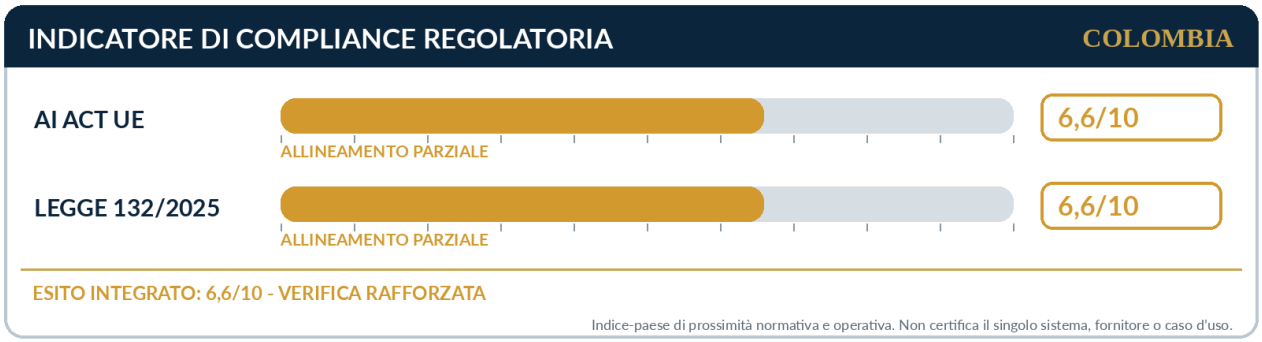
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Cipro del Nord: World Development Indicators, valori più recenti disponibili 2022-2024; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Bassa con copertura 0/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Colombia

Posizione FOTR	56	Area	Americhe	Subregione	America meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	6,6	GCRI / 10	6,5	Classe operativa	Affidabilità favorevole ma condizionata

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Colombia, AI Act UE 6,6/10; legge 132/2025 6,6/10; esito integrato 6,6/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Americhe, Colombia presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 69/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,5/10) e indice FOTR (6,6/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. In Colombia la trasformazione digitale procede più rapidamente dell'uniformità regolatoria e operativa. Gli investimenti devono essere accompagnati da audit, clausole di uscita e gestione locale del rischio.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	79,3% / 17,2 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	98,9% / 1.126 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	77,9 / 81,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	65,9/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	59,6/100 - rank 64	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	64/100 - Parzialmente libero / Libero (69/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,0 / 5,5 / 6,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Colombia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Colombia le evidenze principali sono GTMI 81,7/100, EGDI 77,9/100, GCI 65,9/100, AI readiness 59,6/100. La dimensione più robusta è maturità infrastrutturale (7,3/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,9/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Colombia è 7,3/10. La base statistica rileva utenti Internet pari al 79,3% nel 2024; 17,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 98,9% nel 2024; 1.126 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Colombia al posto 64 con un valore medio di 59,6/100; il pilastro migliore è politiche pubbliche (80,5/100), quello più debole è sviluppo e diffusione (35,3/100). Il GTMI 2025 è 81,7/100. Il punteggio S2 è 6,5/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Colombia è valutata sufficiente ma disomogenea, con S3 pari a 6,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 77,9/100, sviluppo e diffusione dell'IA 35,3/100, penetrazione Internet 79,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Colombia ottiene S4 5,9/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Colombia, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla valutazione è misurato da S4=5,9/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Colombia è S5 6,5/10. La base ITU registra ITU GCI 65,9/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è cooperazione (10,2/20). Freedom on the Net è 64/100 - Parzialmente libero, mentre Freedom in the World è Libero (69/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge 1581/2012, decreti attuativi e supervisione SIC; trasferimenti internazionali da valutare con clausole, base giuridica e controllo della catena dei responsabili.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,0	Crimini finanziari	8,0
Reti criminali	9,5	Attori incorporati nello Stato	7,5
Attori stranieri	7,5	Attori del settore privato	7,0
Resilienza complessiva	5,5	Cooperazione internazionale	9,0
Politiche e norme nazionali	6,5	Forze dell'ordine	4,5
Antiriciclaggio	6,0	Prevenzione	4,5
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	6,9 - ALTO

Quadro criminale digitale. Per Colombia, l'indice operativo FOTR-CY è 6,9/10, classe alta. Il mercato dei reati cyber-dipendenti è elevato (7,0/10), mentre i crimini finanziari sono molto elevati (8,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (9,5/10) e attori incorporati nello Stato (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Colombia assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Colombia, la resilienza complessiva è debole (5,5/10); la cooperazione internazionale è robusta (9,0/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 4,5/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Colombia, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Colombia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Colombia, In Colombia le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Colombia, Il livello governativo di Colombia presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Colombia, Sul piano militare e dual-use, Colombia mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Colombia, Legge 1581/2012, decreti attuativi e supervisione SIC; trasferimenti internazionali da valutare con clausole, base giuridica e controllo della catena dei responsabili. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Colombia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 6,4/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,3	6,5	6,4	5,9	6,5	6,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,7	6,6	6,3	7,0	6,6	6,4

Il GCRI di Colombia è 6,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (7,0/10), mentre il più basso è Trasparenza istituzionale (6,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Colombia, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Colombia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Colombia, Dal punto di vista italiano, Colombia rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Colombia è favorevole ma condizionata: il valore FOTR di 6,6/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Trasparenza istituzionale.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

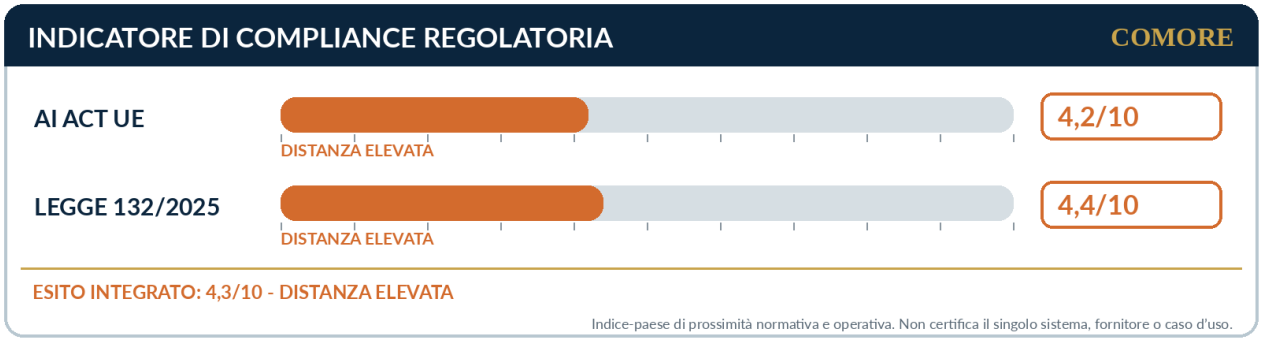
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Colombia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Comore

Posizione FOTR	145	Area	Africa	Subregione	Africa centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,5	GCRI / 10	3,2	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Comore, AI Act UE 4,2/10; legge 132/2025 4,4/10; esito integrato 4,3/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Comore, situato in Africa centrale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 41/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (4,5/10) supera il GCRI tecnico (3,2/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Per Comore non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	32,5% / 0,4 per 100	2024/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	91,7% / 16 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	25,9 / 18,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	39,2/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	20,3/100 - rank 171	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (41/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 2,6 / 4,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Comore, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Comore le evidenze principali sono GTMI 18,6/100, EGDI 25,9/100, GCI 39,2/100, AI readiness 20,3/100. La dimensione più robusta è postura di sicurezza cyber (4,1/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (1,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Comore è 3,4/10. La base statistica rileva utenti Internet pari al 32,5% nel 2024; 0,4 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 91,7% nel 2024; 16 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Comore al posto 171 con un valore medio di 20,3/100; il pilastro migliore è adozione pubblica (34,5/100), quello più debole è politiche pubbliche (7,5/100). Il GTMI 2025 è 18,6/100. Il punteggio S2 è 1,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Comore è valutata fragile, con S3 pari a 2,9/10. Le evidenze disponibili comprendono indice UN di capitale umano 39,9/100, sviluppo e diffusione dell'IA 10,0/100, penetrazione Internet 32,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Comore ottiene S4 3,9/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Comore, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=3,9/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Comore è S5 4,1/10. La base ITU registra ITU GCI 39,2/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è cooperazione (1,5/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (41/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	5,5
Reti criminali	4,5	Attori incorporati nello Stato	7,0
Attori stranieri	5,0	Attori del settore privato	2,0
Resilienza complessiva	2,6	Cooperazione internazionale	3,0
Politiche e norme nazionali	2,5	Forze dell'ordine	2,5
Antiriciclaggio	4,0	Prevenzione	2,5
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	4,9 - MODERATO

Sintesi del rischio cybercrime. Comore presenta un'esposizione stimata moderata (4,9/10): reati cyber-dipendenti 2,0/10, crimini finanziari 5,5/10 e resilienza 2,6/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,0/10) e attori stranieri (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Comore assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Comore, la resilienza complessiva è molto debole (2,6/10); la cooperazione internazionale è molto debole (3,0/10), le politiche e norme nazionali sono molto deboli (2,5/10) e la capacità delle forze dell'ordine è molto debole (2,5/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 2,5/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Comore, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Comore. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Comore, In Comore le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Comore, Il livello governativo di Comore presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Comore, Sul piano militare e dual-use, Comore mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Comore, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Comore, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,4/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,4	1,9	2,9	3,9	4,1	3,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,3	4,3	4,6	5,1	4,0	4,4

Il GCRI di Comore è 3,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,1/10), mentre il più basso è Supply chain (4,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Comore, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Comore, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Comore, Dal punto di vista italiano, Comore rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Comore ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.
Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

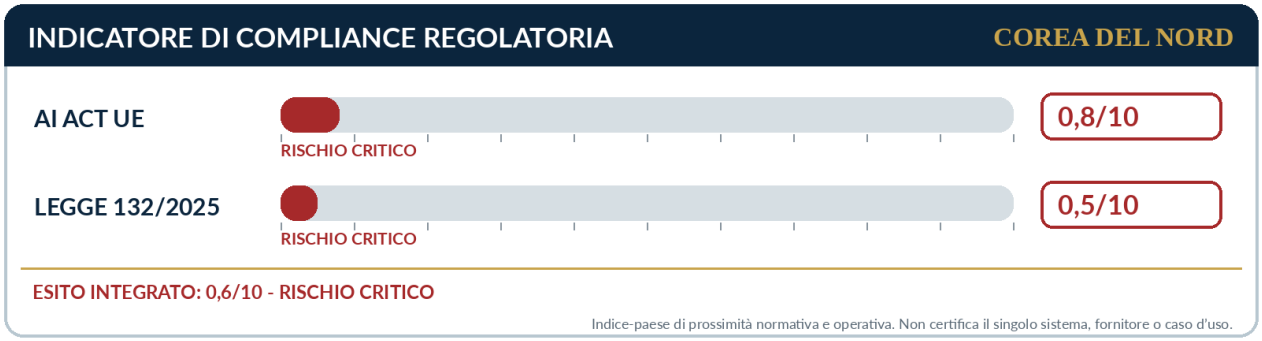
Profilo Celeborn Intelligence di Comore: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.



Corea del Nord

Posizione FOTR	208	Area	Asia	Subregione	Asia orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Media	Copertura dati	5/7 famiglie
FOTR / 10	0,2	GCRI / 10	3,3	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Corea del Nord, AI Act UE 0,8/10; legge 132/2025 0,5/10; esito integrato 0,6/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

La Corea del Nord presenta un ecosistema digitale chiuso, fortemente controllato e orientato a finalità statali e militari. La limitata accessibilità pubblica delle reti non implica bassa capacità offensiva: le fonti aperte descrivono una notevole asimmetria tra connettività della popolazione e risorse dedicate alle operazioni cyber. Per l'Italia la regola operativa è la non cooperazione, salvo attività umanitarie o istituzionali espressamente autorizzate e completamente segregate. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 3/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (3,3/10) è superiore al punteggio FOTR (0,2/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Il rapporto digitale con Corea del Nord deve essere considerato eccezionale e ad alta esposizione. Sono necessari screening sanzionatori, autorizzazioni, segregazione completa e impossibilità tecnica di accedere ai dati in chiaro.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	0,0% / n.d. per 100	2004/n.d.	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	61,4% / 10 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	23,2 / 1,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	6,2/100 - Tier 5 - capacità iniziali	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	80,5/100 - rank 5	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (3/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	9,0 / 1,6 / 7,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Corea del Nord, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 5/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Corea del Nord le evidenze principali sono GTMI 1,0/100, EGDI 23,2/100, GCI 6,2/100, AI readiness 80,5/100. La dimensione più robusta è adozione di IA e tecnologie emergenti (5,4/10), mentre la criticità relativa riguarda postura di sicurezza cyber (0,7/10). Sono disponibili 5 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata media. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Corea del Nord è 1,9/10. La base statistica rileva utenti Internet pari al 0,0% nel 2004; accesso all'elettricità del 61,4% nel 2024; 10 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Corea del Nord al posto 5 con un valore medio di 80,5/100; il pilastro migliore è politiche pubbliche (96,0/100), quello più debole è sviluppo e diffusione (65,9/100). Il GTMI 2025 è 1,0/100. Il punteggio S2 è 5,4/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Corea del Nord è valutata sufficiente ma disomogenea, con S3 pari a 5,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 49,2/100, sviluppo e diffusione dell'IA 65,9/100, penetrazione Internet 0,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Corea del Nord ottiene S4 3,4/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Corea del Nord, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo

societario e subfornitura. L'impatto sulla valutazione è misurato da S4=3,4/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Corea del Nord è S5 0,7/10. La base ITU registra ITU GCI 6,2/100, Tier 5 - capacità iniziali; il pilastro relativamente più debole è misure giuridiche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (3/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Sistema integralmente controllato dallo Stato, assenza di rimedi indipendenti e sanzioni internazionali estese; cooperazione digitale ordinaria non praticabile.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	9,0	Crimini finanziari	8,0
Reti criminali	3,0	Attori incorporati nello Stato	10,0
Attori stranieri	4,5	Attori del settore privato	1,0
Resilienza complessiva	1,6	Cooperazione internazionale	2,0
Politiche e norme nazionali	2,0	Forze dell'ordine	1,5
Antiriciclaggio	1,0	Prevenzione	1,0
Supporto vittime e testimoni	1,0	Rischio operativo FOTR-CY	7,9 - ALTO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (9,0/10), criminalità finanziaria (8,0/10) e resilienza (1,6/10) colloca Corea del Nord in una fascia di rischio alto, pari a 7,9/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (10,0/10) e attori stranieri (4,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Corea del Nord assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Corea del Nord, la resilienza complessiva è molto debole (1,6/10); la cooperazione internazionale è molto debole (2,0/10), le politiche e norme nazionali sono molto deboli (2,0/10) e la capacità delle forze dell'ordine è molto debole (1,5/10). Completano il quadro antiriciclaggio 1,0/10, prevenzione 1,0/10 e supporto a vittime e testimoni 1,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Corea del Nord, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Corea del Nord. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Corea del Nord, In Corea del Nord le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o

infrastrutture esterne. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Corea del Nord, Il livello governativo di Corea del Nord presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Corea del Nord, Sul piano militare e dual-use, Corea del Nord mostra forte ruolo statale e integrazione con filiere cinesi o nazionali, con limitata trasparenza esterna. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Corea del Nord, Sistema integralmente controllato dallo Stato, assenza di rimedi indipendenti e sanzioni internazionali estese; cooperazione digitale ordinaria non praticabile. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Corea del Nord, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 0,0/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
1,9	5,4	5,2	3,4	0,7	3,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
0,0	1,3	0,0	0,0	0,4	0,0

Il GCRI di Corea del Nord è 3,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 0,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (1,3/10), mentre il più basso è Compatibilità giuridica (0,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 0,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Corea del Nord, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Corea del Nord, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Corea del Nord, Dal punto di vista italiano, Corea del Nord rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Corea del Nord, il FOTR di 0,2/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

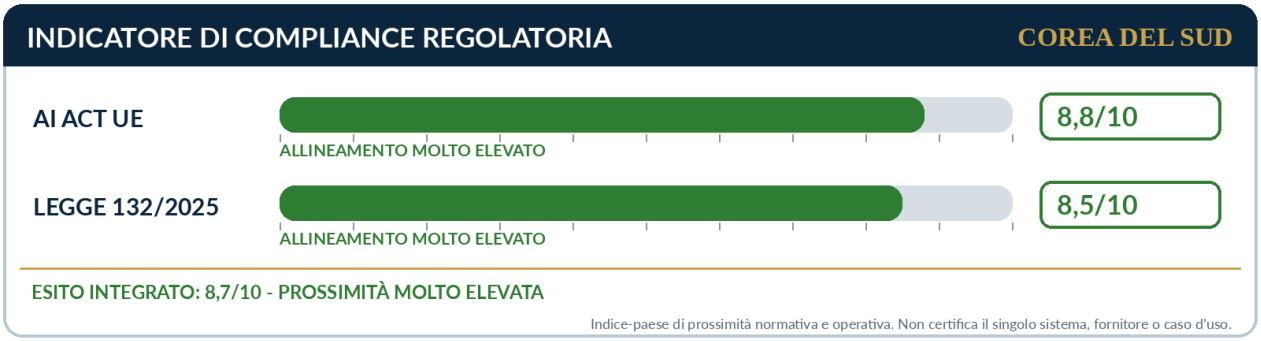
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Corea del Nord: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Media con copertura 5/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Corea del Sud

Posizione FOTR	21	Area	Asia	Subregione	Asia orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	8,7	GCRI / 10	8,7	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Corea del Sud, AI Act UE 8,8/10; legge 132/2025 8,5/10; esito integrato 8,7/10, classe «Allineamento molto elevato». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Corea del Sud è stato membro delle nazioni unite collocato in Asia orientale. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Asia orientale domestica, Stati Uniti, Giappone/Corea. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 83/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,7/10) e indice FOTR (8,7/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Ecosistema tecnologico avanzato, forte industria dei semiconduttori e tutela dati strutturata; cooperazione generalmente favorevole con controllo delle concentrazioni di fornitura.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	97,9% / 47,8 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 11.902 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	96,8 / 99,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	100,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	80,5/100 - rank 5	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	65/100 - Parzialmente libero / Libero (83/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Adeguatezza UE / Firmatario/invitato	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 8,0 / 4,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Corea del Sud, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Corea del Sud le evidenze principali sono GTMI 99,7/100, EGDI 96,8/100, GCI 100,0/100, AI readiness 80,5/100. La dimensione più robusta è maturità infrastrutturale (9,7/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (8,2/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Corea del Sud è 9,7/10. La base statistica rileva utenti Internet pari al 97,9% nel 2024; 47,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 11.902 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Corea del Sud al posto 5 con un valore medio di 80,5/100; il pilastro migliore è politiche pubbliche (96,0/100), quello più debole è sviluppo e diffusione (65,9/100). Il GTMI 2025 è 99,7/100. Il punteggio S2 è 8,5/10 e indica una capacità elevata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Corea del Sud è valutata solida, con S3 pari a 8,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 91,2/100, sviluppo e diffusione dell'IA 65,9/100, penetrazione Internet 97,9%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Corea del Sud ottiene S4 8,3/10 e presenta buona capacità di diversificazione. La provenienza prevalente stimata è Asia orientale domestica, Stati Uniti, Giappone/Corea; l'indicatore di indipendenza disponibile è 8,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Corea del Sud, Fornitura prevalentemente domestica per elettronica e telecomunicazioni, integrata con tecnologie statunitensi e giapponesi. L'impatto sulla valutazione è misurato da S4=8,3/10 e dal proxy di indipendenza 8,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Corea del Sud è S5 8,9/10. La base ITU registra ITU GCI 100,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure giuridiche (20,0/20). Freedom on the Net è 65/100 - Parzialmente libero, mentre Freedom in the World è Libero (83/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Firmatario/invitato. Quadro normativo sintetico: Personal Information Protection Act e disciplina KISA; decisione UE di adeguatezza e forte capacità di enforcement tecnologico.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	4,5
Reti criminali	5,0	Attori incorporati nello Stato	4,0
Attori stranieri	6,5	Attori del settore privato	5,0
Resilienza complessiva	8,0	Cooperazione internazionale	8,5
Politiche e norme nazionali	9,0	Forze dell'ordine	8,0
Antiriciclaggio	8,0	Prevenzione	8,0
Supporto vittime e testimoni	7,0	Rischio operativo FOTR-CY	4,1 - MODERATO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (4,5/10), criminalità finanziaria (4,5/10) e resilienza (8,0/10) colloca Corea del Sud in una fascia di rischio moderato, pari a 4,1/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (6,5/10) e reti criminali (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Corea del Sud assumono particolare rilevanza compromissioni della supply chain, sottrazione di proprietà intellettuale, furto di cripto-attività, phishing mirato, abuso di identità digitali e intrusioni persistenti contro industria e amministrazioni. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Corea del Sud, la resilienza complessiva è robusta (8,0/10); la cooperazione internazionale è robusta (8,5/10), le politiche e norme nazionali sono robuste (9,0/10) e la capacità delle forze dell'ordine è robusta (8,0/10). Completano il quadro antiriciclaggio 8,0/10, prevenzione 8,0/10 e supporto a vittime e testimoni 7,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Corea del Sud, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Corea del Sud. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Corea del Sud, In Corea del Sud le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Corea del Sud, Il livello governativo di Corea del Sud presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Corea del Sud, Sul piano militare e dual-use, Corea del Sud mostra stretta cooperazione con ecosistemi occidentali e capacità dual-use significative. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Corea del Sud, Personal Information Protection Act e disciplina KISA; decisione UE di adeguatezza e forte capacità di enforcement tecnologico. Lo stato rispetto alla Convenzione di Budapest è: Firmatario/invitato; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Corea del Sud, È disponibile una decisione UE di adeguatezza. L'operatore italiano deve comunque controllare la portata della decisione, i trasferimenti successivi, le misure di sicurezza e le eventuali discipline settoriali. La componente FOTR di trasferibilità è 10,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,7	8,5	8,2	8,3	8,9	8,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,0	9,9	7,1	7,6	8,6	10,0

Il GCRI di Corea del Sud è 8,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (10,0/10), mentre il più basso è Trasparenza istituzionale (7,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Corea del Sud, la cautela si concentra su 3 ambiti a rischio intermedio: IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Corea del Sud, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Corea del Sud, Dal punto di vista italiano, Corea del Sud rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Corea del Sud, il FOTR di 8,7/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (7,1/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

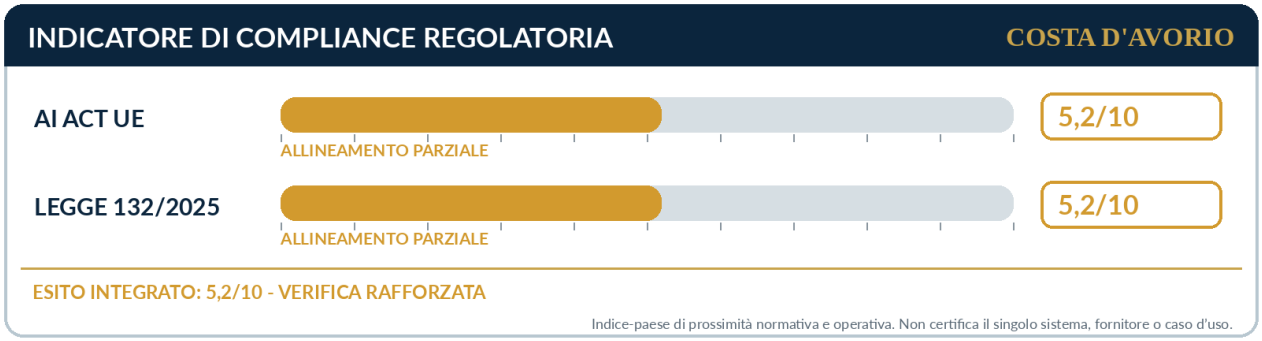
Profilo Celeborn Intelligence di Corea del Sud: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.



Costa d'Avorio

Posizione FOTR	127	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,2	GCRI / 10	5,2	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Costa d'Avorio, AI Act UE 5,2/10; legge 132/2025 5,2/10; esito integrato 5,2/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Costa d'Avorio presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 46/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,2/10) e indice FOTR (5,2/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per Costa d'Avorio non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	41,4% / 1,6 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	72,9% / 61 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	55,9 / 66,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	78,8/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	44,0/100 - rank 95	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (46/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 5,1 / 5,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Costa d'Avorio, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Costa d'Avorio le evidenze principali sono GTMI 66,3/100, EGDI 55,9/100, GCI 78,8/100, AI readiness 44,0/100. La dimensione più robusta è postura di sicurezza cyber (6,9/10), mentre la criticità relativa riguarda maturità infrastrutturale (4,6/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Costa d'Avorio è 4,6/10. La base statistica rileva utenti Internet pari al 41,4% nel 2024; 1,6 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 72,9% nel 2024; 61 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Costa d'Avorio al posto 95 con un valore medio di 44,0/100; il pilastro migliore è governance (60,6/100), quello più debole è adozione pubblica (19,0/100). Il GTMI 2025 è 66,3/100. Il punteggio S2 è 4,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Costa d'Avorio è valutata fragile, con S3 pari a 4,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 48,5/100, sviluppo e diffusione dell'IA 27,9/100, penetrazione Internet 41,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Costa d'Avorio ottiene S4 5,2/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Costa d'Avorio, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre

ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=5,2/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Costa d'Avorio è S5 6,9/10. La base ITU registra ITU GCI 78,8/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (11,1/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (46/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge 2013-450 sulla protezione dei dati e disciplina cyber; ecosistema regionale in crescita con dipendenza da operatori esterni.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	6,5
Reti criminali	6,5	Attori incorporati nello Stato	7,0
Attori stranieri	7,5	Attori del settore privato	5,0
Resilienza complessiva	5,1	Cooperazione internazionale	6,0
Politiche e norme nazionali	6,0	Forze dell'ordine	5,5
Antiriciclaggio	4,5	Prevenzione	5,5
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	5,6 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Costa d'Avorio il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,6/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 4,5/10; le frodi e i reati finanziari 6,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (7,5/10) e attori incorporati nello Stato (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Costa d'Avorio assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Costa d'Avorio, la resilienza complessiva è debole (5,1/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 5,5/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Costa d'Avorio, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Costa d'Avorio. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Costa d'Avorio, In Costa d'Avorio le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi

operatori. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Costa d'Avorio, Il livello governativo di Costa d'Avorio presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Costa d'Avorio, Sul piano militare e dual-use, Costa d'Avorio mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Costa d'Avorio, Legge 2013-450 sulla protezione dei dati e disciplina cyber; ecosistema regionale in crescita con dipendenza da operatori esterni. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Costa d'Avorio, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,2/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
4,6	4,9	4,6	5,2	6,9	5,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,3	5,1	5,0	5,7	5,1	5,2

Il GCRI di Costa d'Avorio è 5,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,7/10), mentre il più basso è Trasparenza istituzionale (5,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 5,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Costa d'Avorio, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Costa d'Avorio, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Costa d'Avorio, Dal punto di vista italiano, Costa d'Avorio rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Costa d'Avorio è indicata una cooperazione selettiva, coerente con il FOTR di 5,2/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

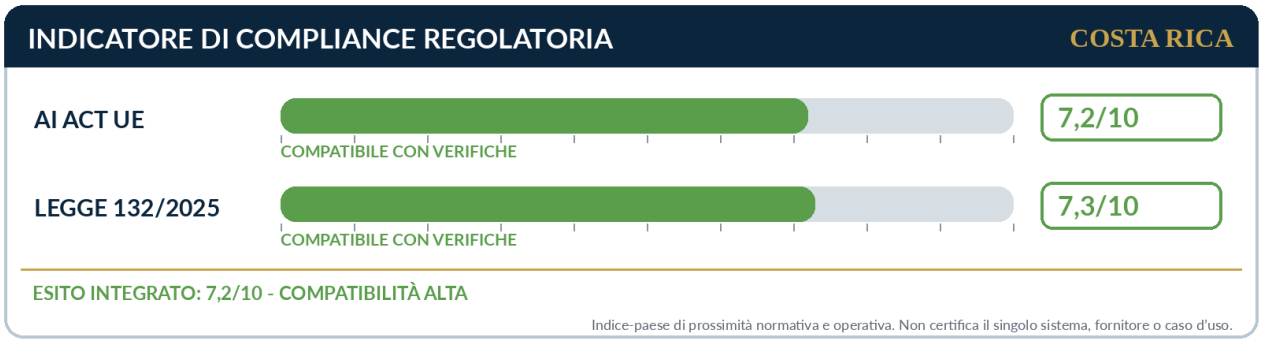
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Costa d'Avorio: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Costa Rica

Posizione FOTR	49	Area	Americhe	Subregione	America centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	7,3	GCRI / 10	6,8	Classe operativa	Affidabilità favorevole ma condizionata

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Costa Rica, AI Act UE 7,2/10; legge 132/2025 7,3/10; esito integrato 7,2/10, classe «Compatibile con verifiche». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Prima dell'ingaggio occorre una analisi degli scostamenti mirata su trasparenza, governance dei dati, rappresentanza nell'UE, audit e rimedi contrattuali.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Costa Rica, situato in America centrale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 91/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,8/10) e indice FOTR (7,3/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Costa Rica combina buona maturità tecnologica e relativa prevedibilità normativa. Il livello di rischio aumenta nei progetti che coinvolgono dati sanitari, identità, infrastrutture critiche o ricerca strategica.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	87,2% / 23,3 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	99,8% / 2.000 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	80,1 / 77,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	75,1/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	50,6/100 - rank 79	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	86/100 - Libero / Libero (91/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,5 / 5,6 / 5,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Costa Rica, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Costa Rica le evidenze principali sono GTMI 77,0/100, EGDI 80,1/100, GCI 75,1/100, AI readiness 50,6/100. La dimensione più robusta è maturità infrastrutturale (8,2/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (5,8/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Costa Rica è 8,2/10. La base statistica rileva utenti Internet pari al 87,2% nel 2024; 23,3 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 99,8% nel 2024; 2.000 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Costa Rica al posto 79 con un valore medio di 50,6/100; il pilastro migliore è politiche pubbliche (69,0/100), quello più debole è sviluppo e diffusione (24,1/100). Il GTMI 2025 è 77,0/100. Il punteggio S2 è 5,8/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Costa Rica è valutata sufficiente ma disomogenea, con S3 pari a 6,3/10. Le evidenze disponibili comprendono indice UN di capitale umano 78,8/100, sviluppo e diffusione dell'IA 24,1/100, penetrazione Internet 87,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Costa Rica ottiene S4 5,9/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Costa Rica, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=5,9/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Costa Rica è S5 7,7/10. La base ITU registra ITU GCI 75,1/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (9,3/20). Freedom on the Net è 86/100 - Libero, mentre Freedom in the World è Libero (91/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge 8968 e regolamento; sistema di protezione dei dati relativamente strutturato, ma senza adeguatezza UE.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,5	Crimini finanziari	6,0
Reti criminali	6,0	Attori incorporati nello Stato	3,5
Attori stranieri	7,5	Attori del settore privato	6,0
Resilienza complessiva	5,6	Cooperazione internazionale	6,5
Politiche e norme nazionali	6,5	Forze dell'ordine	5,0
Antiriciclaggio	4,5	Prevenzione	5,0
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	5,9 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Costa Rica il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,9/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 7,5/10; le frodi e i reati finanziari 6,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (7,5/10) e reti criminali (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Costa Rica assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Costa Rica, la resilienza complessiva è intermedia (5,6/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 5,0/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Costa Rica, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Costa Rica. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Costa Rica, In Costa Rica le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Costa Rica, Il livello governativo di Costa Rica presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Costa Rica, Sul piano militare e dual-use, Costa Rica mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Costa Rica, Legge 8968 e regolamento; sistema di protezione dei dati relativamente strutturato, ma senza adeguatezza UE. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Costa Rica, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 7,0/10 e il rischio sui dati personali è Medio-basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,2	5,8	6,3	5,9	7,7	6,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
7,5	7,3	7,2	7,4	7,4	7,0

Il GCRI di Costa Rica è 6,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 7,3/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (7,5/10), mentre il più basso è Trasferibilità dati (7,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 7,3/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Costa Rica, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Costa Rica, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Costa Rica, Dal punto di vista italiano, Costa Rica rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Costa Rica è favorevole ma condizionata: il valore FOTR di 7,3/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Trasferibilità dati.

Presidi minimi raccomandati

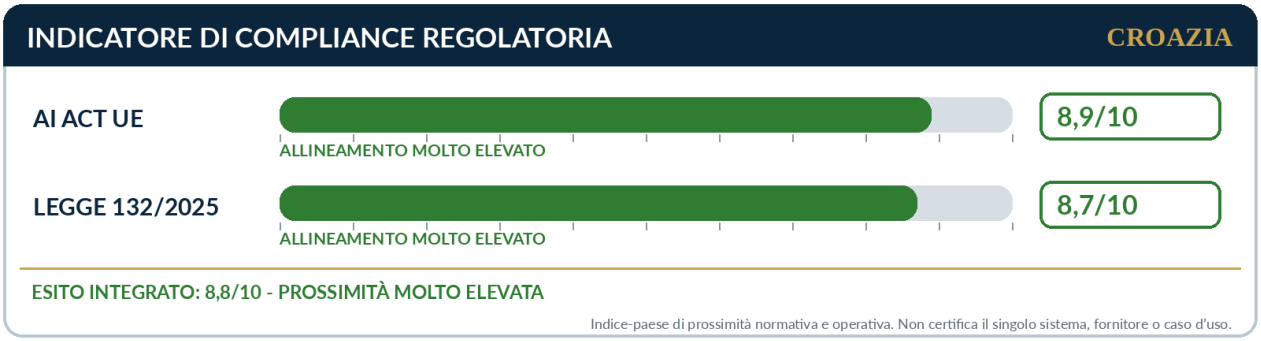
Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Costa Rica: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Croazia

Posizione FOTR	35	Area	Europa	Subregione	Europa sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,1	GCRI / 10	7,2	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Croazia, AI Act UE 8,9/10; legge 132/2025 8,7/10; esito integrato 8,8/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Per un operatore italiano, Croazia non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 82/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,2/10) e indice FOTR (8,1/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ambiente digitale di Croazia è complessivamente affidabile e aperto agli scambi. Per investimenti italiani è opportuno verificare la disciplina locale, la struttura dei fornitori e gli eventuali poteri pubblici di accesso.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	83,6% / 29,6 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 29.459 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	88,2 / 77,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	87,8/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	50,6/100 - rank 72	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (82/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 5,9 / 5,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Croazia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Croazia le evidenze principali sono GTMI 77,4/100, EGDI 88,2/100, GCI 87,8/100, AI readiness 50,6/100. La dimensione più robusta è maturità infrastrutturale (8,7/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Croazia è 8,7/10. La base statistica rileva utenti Internet pari al 83,6% nel 2024; 29,6 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 29.459 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Croazia al posto 72 con un valore medio di 50,6/100; il pilastro migliore è adozione pubblica (71,7/100), quello più debole è sviluppo e diffusione (29,9/100). Il GTMI 2025 è 77,4/100. Il punteggio S2 è 6,1/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Croazia è valutata sufficiente ma disomogenea, con S3 pari a 6,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 85,4/100, sviluppo e diffusione dell'IA 29,9/100, penetrazione Internet 83,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Croazia ottiene S4 5,9/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Croazia, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=5,9/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Croazia è S5 8,4/10. La base ITU registra ITU GCI 87,8/100, Tier 2 - avanzato; il pilastro relativamente più debole è cooperazione (14,3/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (82/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, legge nazionale di attuazione e disciplina di cybersicurezza coerente con NIS2 e CER.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	6,0
Reti criminali	6,0	Attori incorporati nello Stato	6,0
Attori stranieri	5,0	Attori del settore privato	5,0
Resilienza complessiva	5,9	Cooperazione internazionale	7,0
Politiche e norme nazionali	7,0	Forze dell'ordine	6,0
Antiriciclaggio	6,5	Prevenzione	6,0
Supporto vittime e testimoni	6,0	Rischio operativo FOTR-CY	5,1 - SIGNIFICATIVO

Quadro criminale digitale. Per Croazia, l'indice operativo FOTR-CY è 5,1/10, classe significativa. Il mercato dei reati cyber-dipendenti è intermedio (5,0/10), mentre i crimini finanziari sono elevati (6,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (6,0/10) e attori incorporati nello Stato (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Croazia assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Croazia, la resilienza complessiva è intermedia (5,9/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è intermedia (6,0/10). Completano il quadro antiriciclaggio 6,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 6,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Croazia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Croazia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Croazia, In Croazia le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Croazia, Il livello governativo di Croazia presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Croazia, Sul piano militare e dual-use, Croazia mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Croazia, GDPR, legge nazionale di attuazione e disciplina di cybersicurezza coerente con NIS2 e CER. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Croazia, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,1/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,7	6,1	6,8	5,9	8,4	7,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,6	7,9	7,1	8,6	7,2	9,1

Il GCRI di Croazia è 7,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,1/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,1/10), mentre il più basso è Trasparenza istituzionale (7,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,1/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Croazia, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Croazia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Croazia, Dal punto di vista italiano, Croazia rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Croazia, il FOTR di 8,1/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (7,1/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

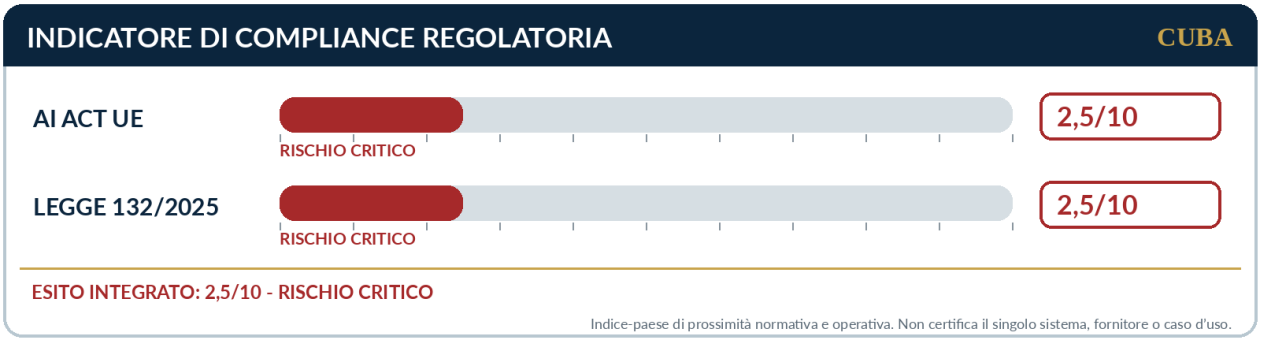
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Croazia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Cuba

Posizione FOTR	187	Area	Americhe	Subregione	Caraibi
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	2,4	GCRI / 10	4,4	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Cuba, AI Act UE 2,5/10; legge 132/2025 2,5/10; esito integrato 2,5/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Cuba è stato membro delle nazioni unite collocato in Caraibi. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina, Russia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 9/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (4,4/10) è superiore al punteggio FOTR (2,4/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Per Cuba la regola operativa è evitare trasferimenti e dipendenze tecnologiche, salvo finalità umanitarie o istituzionali autorizzate e protette da architetture isolate. Il contratto, da solo, non rende il rischio accettabile.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	70,5% / 3,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 193 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	49,2 / 43,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	72,7/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	30,7/100 - rank 136	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	21/100 - Non libero / Non libero (9/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 5,0 / 3,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Cuba, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Cuba le evidenze principali sono GTMI 43,2/100, EGDI 49,2/100, GCI 72,7/100, AI readiness 30,7/100. La dimensione più robusta è maturità infrastrutturale (5,4/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,2/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Cuba è 5,4/10. La base statistica rileva utenti Internet pari al 70,5% nel 2024; 3,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 193 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Cuba al posto 136 con un valore medio di 30,7/100; il pilastro migliore è resilienza (48,3/100), quello più debole è adozione pubblica (4,5/100). Il GTMI 2025 è 43,2/100. Il punteggio S2 è 3,2/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Cuba è valutata fragile, con S3 pari a 4,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 71,5/100, sviluppo e diffusione dell'IA 17,3/100, penetrazione Internet 70,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Cuba ottiene S4 3,9/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina, Russia; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Cuba, Forniture statali, cinesi e russe, con accesso limitato a ecosistemi occidentali. L'impatto sulla valutazione è misurato da S4=3,9/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Cuba è S5 5,0/10. La base ITU registra ITU GCI 72,7/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è cooperazione (6,9/20). Freedom on the Net è 21/100 - Non libero, mentre Freedom in the World è Non libero (9/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Regime statale delle telecomunicazioni e normativa sulla protezione dei dati in un ambiente fortemente controllato; sanzioni e rimedi limitati.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	3,5
Reti criminali	3,0	Attori incorporati nello Stato	3,5
Attori stranieri	2,0	Attori del settore privato	4,5
Resilienza complessiva	5,0	Cooperazione internazionale	6,5
Politiche e norme nazionali	5,5	Forze dell'ordine	6,0
Antiriciclaggio	5,5	Prevenzione	6,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	3,7 - MODERATO

Rischio criminale connesso alle tecnologie. In Cuba il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 3,7/10, livello moderato. I reati che dipendono direttamente da sistemi informatici raggiungono 3,0/10; le frodi e i reati finanziari 3,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori del settore privato (4,5/10) e attori incorporati nello Stato (3,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Cuba assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Cuba, la resilienza complessiva è debole (5,0/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è intermedia (6,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Cuba, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Cuba. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Cuba, In Cuba le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Cuba, Il livello governativo di Cuba presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Cuba, Sul piano militare e dual-use, Cuba mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Cuba, Regime statale delle telecomunicazioni e normativa sulla protezione dei dati in un ambiente fortemente controllato; sanzioni e rimedi limitati. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Cuba, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 1,5/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
5,4	3,2	4,5	3,9	5,0	4,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
2,7	4,1	1,5	1,2	3,5	1,5

Il GCRI di Cuba è 4,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 2,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (4,1/10), mentre il più basso è Compatibilità strategica (1,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Alto	Alto	Estremo	Alto	Estremo

La matrice applica il FOTR di 2,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Cuba, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Cuba, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Cuba, Dal punto di vista italiano, Cuba rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Cuba, il FOTR di 2,4/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

- Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.
- Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.
- Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.
- Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

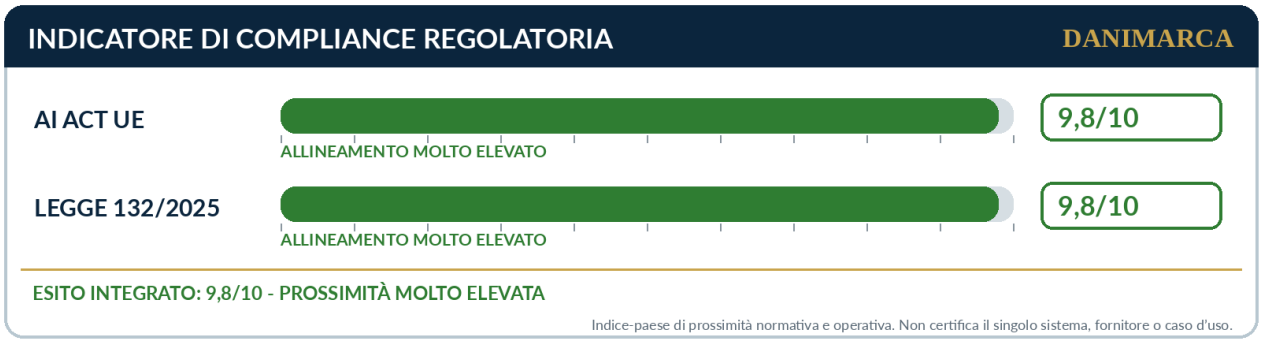
Profilo Celeborn Intelligence di Cuba: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom

House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Danimarca

Posizione FOTR	**1**	**Area**	Europa	**Subregione**	Europa settentrionale e baltica
Status	**Stato membro delle Nazioni Unite**	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	**9,6**	**GCRI / 10**	**8,6**	**Classe operativa**	**Affidabilità molto alta**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Danimarca, AI Act UE 9,8/10; legge 132/2025 9,8/10; esito integrato 9,8/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Nel quadro di Europa, Danimarca presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 97/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (9,6/10) supera il GCRI tecnico (8,6/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il sistema digitale di Danimarca è avanzato e integrato con standard internazionali. Le principali criticità non sono di base istituzionale, ma riguardano supply chain, concentrazione dei servizi e gestione delle eccezioni di sicurezza nazionale.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	99,8% / 43,4 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 246.546 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	98,5 / 92,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	100,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	80,0/100 - rank 11	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (97/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,5 / 8,2 / 4,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Danimarca, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Danimarca le evidenze principali sono GTMI 92,8/100, EGDI 98,5/100, GCI 100,0/100, AI readiness 80,0/100. La dimensione più robusta è maturità infrastrutturale (10,0/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,6/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Danimarca è 10,0/10. La base statistica rileva utenti Internet pari al 99,8% nel 2024; 43,4 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 246.546 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Danimarca al posto 11 con un valore medio di 80,0/100; il pilastro migliore è governance (94,0/100), quello più debole è sviluppo e diffusione (58,9/100). Il GTMI 2025 è 92,8/100. Il punteggio S2 è 8,3/10 e indica una capacità elevata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Danimarca è valutata solida, con S3 pari a 8,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 95,8/100, sviluppo e diffusione dell'IA 58,9/100, penetrazione Internet 99,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Danimarca ottiene S4 6,6/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open

source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Danimarca, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario, luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,6/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Danimarca è S5 9,7/10. La base ITU registra ITU GCI 100,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure giuridiche (20,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (97/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, Danish Data Protection Act e disciplina settoriale cyber; applicazione del quadro UE, con amministrazione digitale molto integrata.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,5	Crimini finanziari	5,5
Reti criminali	5,0	Attori incorporati nello Stato	1,5
Attori stranieri	5,5	Attori del settore privato	2,5
Resilienza complessiva	8,2	Cooperazione internazionale	8,0
Politiche e norme nazionali	9,0	Forze dell'ordine	8,0
Antiriciclaggio	7,0	Prevenzione	8,5
Supporto vittime e testimoni	7,5	Rischio operativo FOTR-CY	4,4 - MODERATO

Pressione del crimine digitale. Il profilo di Danimarca restituisce un rischio FOTR-CY di 4,4/10 (moderato). La componente cyber-dipendente vale 6,5/10 e quella finanziaria 5,5/10; la risposta sistemica è valutata robusta, con resilienza media di 8,2/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (5,5/10) e reti criminali (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Danimarca assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Danimarca, la resilienza complessiva è robusta (8,2/10); la cooperazione internazionale è robusta (8,0/10), le politiche e norme nazionali sono robuste (9,0/10) e la capacità delle forze dell'ordine è robusta (8,0/10). Completano il quadro antiriciclaggio 7,0/10, prevenzione 8,5/10 e supporto a vittime e testimoni 7,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Danimarca, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Danimarca. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Danimarca, In Danimarca le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La

disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Danimarca, Il livello governativo di Danimarca presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Danimarca, Sul piano militare e dual-use, Danimarca mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Danimarca, GDPR, Danish Data Protection Act e disciplina settoriale cyber; applicazione del quadro UE, con amministrazione digitale molto integrata. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Danimarca, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 10,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
10,0	8,3	8,6	6,6	9,7	8,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
10,0	9,1	9,4	10,0	8,9	10,0

Il GCRI di Danimarca è 8,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 9,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (10,0/10), mentre il più basso è Supply chain (8,9/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Basso	Basso	Basso

La matrice applica il FOTR di 9,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Danimarca, la matrice non individua ambiti ad alto rischio; 6 categorie risultano basse o medio-basse, ferma la verifica del singolo progetto. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Danimarca, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Danimarca, Dal punto di vista italiano, Danimarca rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Danimarca, il FOTR di 9,6/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (8,9/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

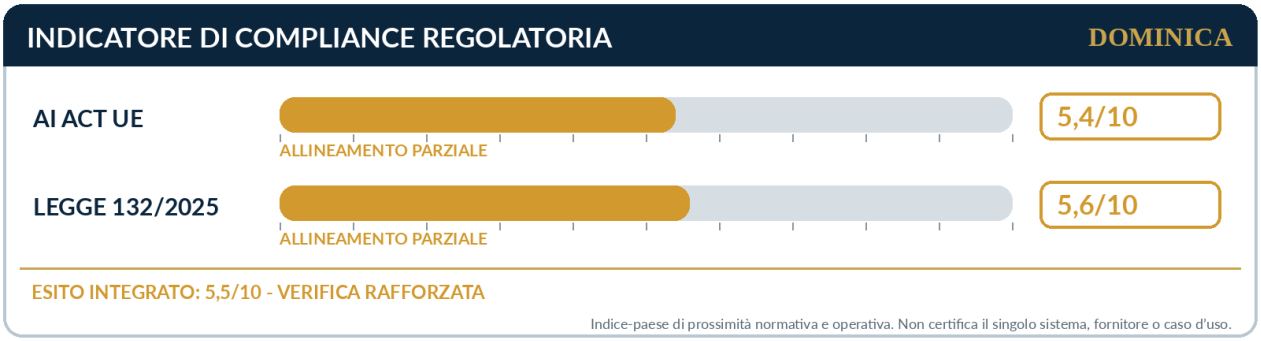
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Danimarca: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Dominica

Posizione FOTR	95	Area	Americhe	Subregione	Caraibi
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,7	GCRI / 10	4,3	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Dominica, AI Act UE 5,4/10; legge 132/2025 5,6/10; esito integrato 5,5/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Dominica, situato in Caraibi, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 92/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,7/10) supera il GCRI tecnico (4,3/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il quadro di Dominica è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	82,0% / 20,9 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 62.865 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	54,5 / 32,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	22,8/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	18,2/100 - rank 174	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (92/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 5,3 / 3,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Dominica, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Dominica le evidenze principali sono GTMI 32,2/100, EGDI 54,5/100, GCI 22,8/100, AI readiness 18,2/100. La dimensione più robusta è maturità infrastrutturale (7,6/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,5/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Dominica è 7,6/10. La base statistica rileva utenti Internet pari al 82,0% nel 2024; 20,9 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 100,0% nel 2024; 62.865 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Dominica al posto 174 con un valore medio di 18,2/100; il pilastro migliore è infrastrutture IA (34,5/100), quello più debole è politiche pubbliche (4,0/100). Il GTMI 2025 è 32,2/100. Il punteggio S2 è 2,5/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Dominica è valutata fragile, con S3 pari a 4,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 57,8/100, sviluppo e diffusione dell'IA 12,9/100, penetrazione Internet 82,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Dominica ottiene S4 4,2/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Dominica, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=4,2/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Dominica è S5 3,4/10. La base ITU registra ITU GCI 22,8/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (92/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	4,0
Reti criminali	4,0	Attori incorporati nello Stato	2,0
Attori stranieri	2,5	Attori del settore privato	1,5
Resilienza complessiva	5,3	Cooperazione internazionale	7,0
Politiche e norme nazionali	5,0	Forze dell'ordine	5,5
Antiriciclaggio	5,5	Prevenzione	6,0
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	3,2 - MODERATO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (2,0/10), criminalità finanziaria (4,0/10) e resilienza (5,3/10) colloca Dominica in una fascia di rischio moderato, pari a 3,2/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (4,0/10) e attori stranieri (2,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Dominica assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Dominica, la resilienza complessiva è debole (5,3/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Dominica, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Dominica. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Dominica, In Dominica le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Dominica, Il livello governativo di Dominica presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il

settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Dominica, Sul piano militare e dual-use, Dominica mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Dominica, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Dominica, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,7/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,6	2,5	4,0	4,2	3,4	4,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,8	5,3	5,8	6,3	5,3	5,7

Il GCRI di Dominica è 4,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,3/10), mentre il più basso è Maturità cyber (5,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Dominica, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Dominica, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Dominica, Dal punto di vista italiano, Dominica rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Dominica è indicata una cooperazione selettiva, coerente con il FOTR di 5,7/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Maturità cyber a decisione caso per caso.

Presidi minimi raccomandati

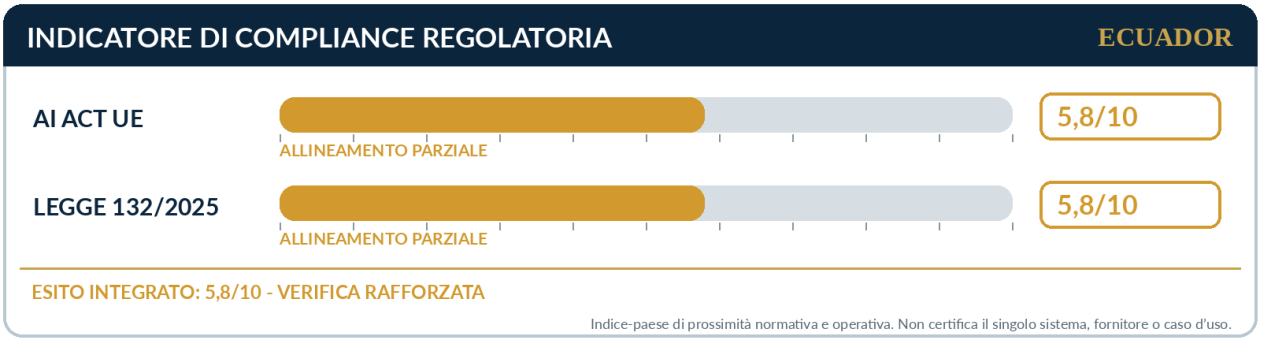
Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Dominica: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Ecuador

Posizione FOTR	96	Area	Americhe	Subregione	America meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,7	GCRI / 10	6,4	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Ecuador, AI Act UE 5,8/10; legge 132/2025 5,8/10; esito integrato 5,8/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Ecuador non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 64/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,4/10) e indice FOTR (5,7/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Ecuador dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	77,2% / 17,2 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	98,5% / 491 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	78,0 / 82,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	87,2/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	57,8/100 - rank 66	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	63/100 - Parzialmente libero / Parzialmente libero (64/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,0 / 4,5 / 6,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Ecuador, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Ecuador le evidenze principali sono GTMI 82,2/100, EGDI 78,0/100, GCI 87,2/100, AI readiness 57,8/100. La dimensione più robusta è postura di sicurezza cyber (7,3/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,6/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Ecuador è 6,8/10. La base statistica rileva utenti Internet pari al 77,2% nel 2024; 17,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 98,5% nel 2024; 491 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Ecuador al posto 66 con un valore medio di 57,8/100; il pilastro migliore è adozione pubblica (79,3/100), quello più debole è sviluppo e diffusione (27,9/100). Il GTMI 2025 è 82,2/100. Il punteggio S2 è 6,5/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Ecuador è valutata sufficiente ma disomogenea, con S3 pari a 6,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 77,1/100, sviluppo e diffusione dell'IA 27,9/100, penetrazione Internet 77,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Ecuador ottiene S4 5,6/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Ecuador, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla valutazione è misurato da S4=5,6/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Ecuador è S5 7,3/10. La base ITU registra ITU GCI 87,2/100, Tier 2 - avanzato; il pilastro relativamente più debole è sviluppo delle capacità (13,8/20). Freedom on the Net è 63/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (64/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,0	Crimini finanziari	7,0
Reti criminali	8,5	Attori incorporati nello Stato	7,5
Attori stranieri	8,0	Attori del settore privato	7,0
Resilienza complessiva	4,5	Cooperazione internazionale	6,5
Politiche e norme nazionali	5,0	Forze dell'ordine	4,0
Antiriciclaggio	5,0	Prevenzione	4,0
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	6,9 - ALTO

Quadro criminale digitale. Per Ecuador, l'indice operativo FOTR-CY è 6,9/10, classe alta. Il mercato dei reati cyber-dipendenti è elevato (7,0/10), mentre i crimini finanziari sono elevati (7,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (8,5/10) e attori stranieri (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Ecuador assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Ecuador, la resilienza complessiva è debole (4,5/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Ecuador, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Ecuador. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Ecuador, In Ecuador le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Ecuador, Il livello governativo di Ecuador presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Ecuador, Sul piano militare e dual-use, Ecuador mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Ecuador, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Ecuador, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,6/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,8	6,5	6,0	5,6	7,3	6,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,6	5,7	5,5	6,2	5,9	5,6

Il GCRI di Ecuador è 6,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,2/10), mentre il più basso è Trasparenza istituzionale (5,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Ecuador, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Ecuador, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Ecuador, Dal punto di vista italiano, Ecuador rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Ecuador è indicata una cooperazione selettiva, coerente con il FOTR di 5,7/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasparenza istituzionale a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

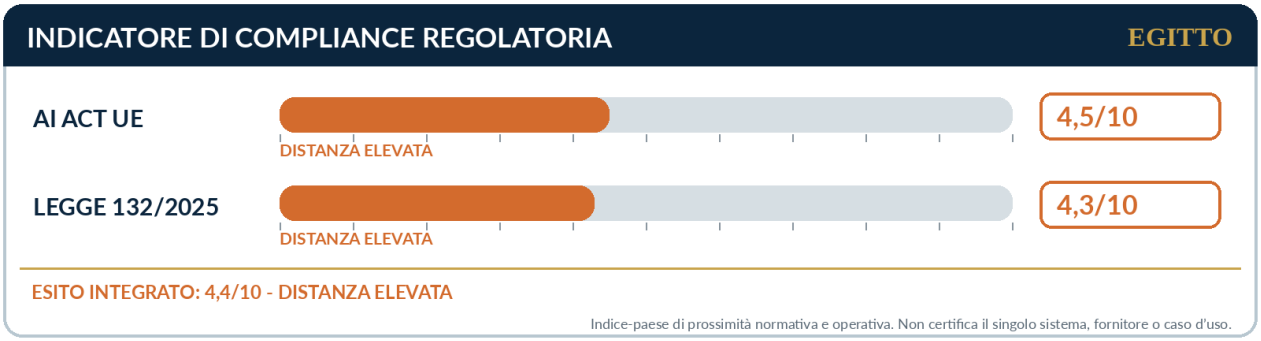
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Ecuador: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Egitto

Posizione FOTR	172	Area	Africa	Subregione	Africa settentrionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	4,2	GCRI / 10	6,1	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Egitto, AI Act UE 4,5/10; legge 132/2025 4,3/10; esito integrato 4,4/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Egitto è stato membro delle nazioni unite collocato in Africa settentrionale. La partecipazione al coordinamento BRICS segnala una strategia di autonomia e diversificazione rispetto agli ecosistemi occidentali, con relazioni tecnologiche più intense verso Cina, Russia o altri poli emergenti. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, Russia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 18/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (6,1/10) è superiore al punteggio FOTR (4,2/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Egitto è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	74,6% / 11,7 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 82 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	67,0 / 91,1	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	100,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	64,0/100 - rank 52	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	28/100 - Non libero / Non libero (18/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 3,8 / 5,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Egitto, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Egitto le evidenze principali sono GTMI 91,1/100, EGDI 67,0/100, GCI 100,0/100, AI readiness 64,0/100. La dimensione più robusta è adozione di IA e tecnologie emergenti (6,9/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,1/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Egitto è 6,3/10. La base statistica rileva utenti Internet pari al 74,6% nel 2024; 11,7 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 82 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Egitto al posto 52 con un valore medio di 64,0/100; il pilastro migliore è politiche pubbliche (100,0/100), quello più debole è sviluppo e diffusione (47,7/100). Il GTMI 2025 è 91,1/100. Il punteggio S2 è 6,9/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Egitto è valutata sufficiente ma disomogenea, con S3 pari a 5,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 61,5/100, sviluppo e diffusione dell'IA 47,7/100, penetrazione Internet 74,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Egitto ottiene S4 5,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, Russia; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Egitto, Fornitori europei, statunitensi, cinesi e russi, con forte controllo e coordinamento statale. L'impatto sulla valutazione è misurato da S4=5,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Egitto è S5 6,7/10. La base ITU registra ITU GCI 100,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure giuridiche (20,0/20). Freedom on the Net è 28/100 - Non libero, mentre Freedom in the World è Non libero (18/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Personal Data Protection Law 151/2020, Telecom Law e poteri di sicurezza estesi; licenze, localizzazione e accessi pubblici richiedono cautela.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	8,0
Reti criminali	6,0	Attori incorporati nello Stato	8,5
Attori stranieri	5,0	Attori del settore privato	3,5
Resilienza complessiva	3,8	Cooperazione internazionale	5,0
Politiche e norme nazionali	4,5	Forze dell'ordine	5,0
Antiriciclaggio	5,0	Prevenzione	2,5
Supporto vittime e testimoni	2,5	Rischio operativo FOTR-CY	5,6 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Egitto restituisce un rischio FOTR-CY di 5,6/10 (significativo). La componente cyber-dipendente vale 3,0/10 e quella finanziaria 8,0/10; la risposta sistemica è valutata debole, con resilienza media di 3,8/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,5/10) e reti criminali (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Egitto assumono particolare rilevanza phishing e credential theft, ransomware, frodi d'investimento, attacchi a energia e servizi pubblici, abuso di cripto-attività e campagne che possono combinare profitto, spionaggio e pressione politica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Egitto, la resilienza complessiva è debole (3,8/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono deboli (4,5/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 2,5/10 e supporto a vittime e testimoni 2,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Egitto, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Egitto. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Egitto, In Egitto le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Egitto, Il livello governativo di Egitto presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Egitto, Sul piano militare e dual-use, Egitto mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Egitto, Personal Data Protection Law 151/2020, Telecom Law e poteri di sicurezza estesi; licenze, localizzazione e accessi pubblici richiedono cautela. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Egitto, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,3/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,3	6,9	5,6	5,1	6,7	6,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,2	4,0	4,1	4,6	4,1	4,3

Il GCRI di Egitto è 6,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (4,6/10), mentre il più basso è Maturità cyber (4,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Egitto, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Egitto, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Egitto, Dal punto di vista italiano, Egitto rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Egitto ricade nella fascia di alto rischio (4,2/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

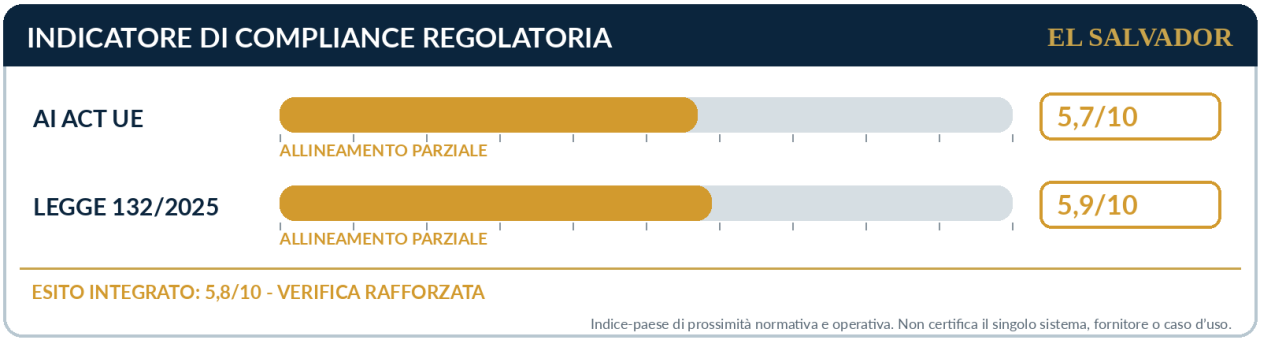
Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.
Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Egitto: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

El Salvador

Posizione FOTR	76	Area	Americhe	Subregione	America centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,9	GCRI / 10	5,2	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di El Salvador, AI Act UE 5,7/10; legge 132/2025 5,9/10; esito integrato 5,8/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Americhe, El Salvador presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 42/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,2/10) e indice FOTR (5,9/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. El Salvador dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	66,5% / 12,5 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	98,7% / 191 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	59,9 / 70,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	37,3/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	40,0/100 - rank 104	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (42/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,5 / 3,2 / 6,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di El Salvador, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per El Salvador le evidenze principali sono GTMI 70,4/100, EGDI 59,9/100, GCI 37,3/100, AI readiness 40,0/100. La dimensione più robusta è maturità infrastrutturale (6,4/10), mentre la criticità relativa riguarda postura di sicurezza cyber (4,5/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di El Salvador è 6,4/10. La base statistica rileva utenti Internet pari al 66,5% nel 2024; 12,5 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 98,7% nel 2024; 191 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca El Salvador al posto 104 con un valore medio di 40,0/100; il pilastro migliore è adozione pubblica (64,2/100), quello più debole è politiche pubbliche (12,0/100). Il GTMI 2025 è 70,4/100. Il punteggio S2 è 4,7/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di El Salvador è valutata fragile, con S3 pari a 4,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 53,5/100, sviluppo e diffusione dell'IA 28,6/100, penetrazione Internet 66,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di El Salvador ottiene S4 5,4/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di El Salvador, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=5,4/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di El Salvador è S5 4,5/10. La base ITU registra ITU GCI 37,3/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,1/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (42/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,5	Crimini finanziari	6,5
Reti criminali	6,0	Attori incorporati nello Stato	7,5
Attori stranieri	5,0	Attori del settore privato	4,5
Resilienza complessiva	3,2	Cooperazione internazionale	4,5
Politiche e norme nazionali	3,5	Forze dell'ordine	3,0
Antiriciclaggio	3,5	Prevenzione	4,0
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	6,5 - ALTO

Pressione del crimine digitale. Il profilo di El Salvador restituisce un rischio FOTR-CY di 6,5/10 (alto). La componente cyber-dipendente vale 6,5/10 e quella finanziaria 6,5/10; la risposta sistemica è valutata molto debole, con resilienza media di 3,2/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,5/10) e reti criminali (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di El Salvador assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di El Salvador, la resilienza complessiva è molto debole (3,2/10); la cooperazione internazionale è debole (4,5/10), le politiche e norme nazionali sono deboli (3,5/10) e la capacità delle forze dell'ordine è molto debole (3,0/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 4,0/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in El Salvador, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di El Salvador. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per El Salvador, In El Salvador le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per El Salvador, Il livello governativo di El Salvador presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per El Salvador, Sul piano militare e dual-use, El Salvador mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per El Salvador, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso El Salvador, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,8/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,4	4,7	4,8	5,4	4,5	5,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,8	5,9	5,8	6,3	5,8	5,8

Il GCRI di El Salvador è 5,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,9/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,3/10), mentre il più basso è Compatibilità giuridica (5,8/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,9/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per El Salvador, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con El Salvador, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e El Salvador, Dal punto di vista italiano, El Salvador rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per El Salvador è indicata una cooperazione selettiva, coerente con il FOTR di 5,9/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Compatibilità giuridica a decisione caso per caso.

Presidi minimi raccomandati

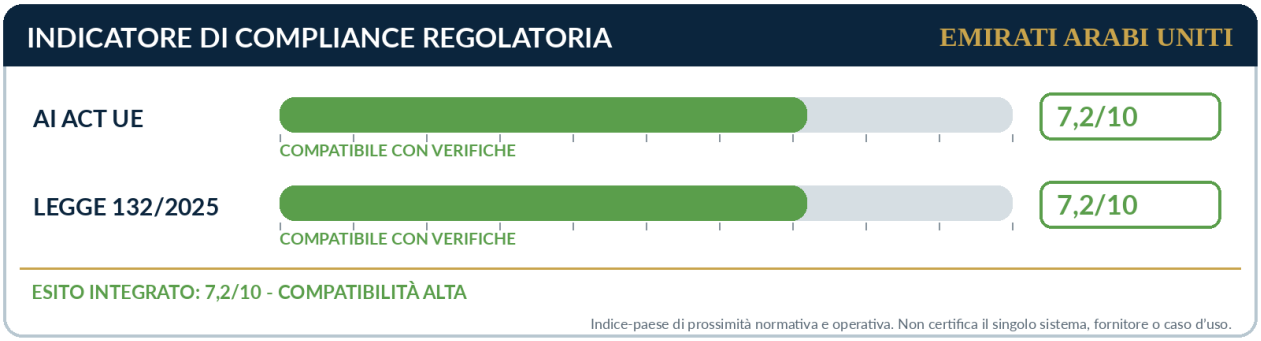
Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di El Salvador: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Emirati Arabi Uniti

Posizione FOTR	**50**	**Area**	Asia	**Subregione**	Medio Oriente e Asia occidentale
Status	**Stato membro delle Nazioni Unite**	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	7/7 famiglie
FOTR / 10	**7,2**	**GCRI / 10**	**8,0**	**Classe operativa**	**Affidabilità favorevole ma condizionata**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Emirati Arabi Uniti, AI Act UE 7,2/10; legge 132/2025 7,2/10; esito integrato 7,2/10, classe «Compatibile con verifiche». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Prima dell'ingaggio occorre una analisi degli scostamenti mirata su trasparenza, governance dei dati, rappresentanza nell'UE, audit e rimedi contrattuali.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Emirati Arabi Uniti, situato in Medio Oriente e Asia occidentale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La partecipazione al coordinamento BRICS segnala una strategia di autonomia e diversificazione rispetto agli ecosistemi occidentali, con relazioni tecnologiche più intense verso Cina, Russia o altri poli emergenti. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 18/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,0/10) e indice FOTR (7,2/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Hub regionale per cloud, IA, finanza e logistica con infrastrutture moderne; la pluralità di regimi giuridici e la centralizzazione richiedono contratti e architetture chiare.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	100,0% / 40,8 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 4.192 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	95,3 / 91,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	100,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	69,5/100 - rank 19	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	28/100 - Non libero / Non libero (18/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	8,0 / 5,1 / 7,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Emirati Arabi Uniti, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Emirati Arabi Uniti le evidenze principali sono GTMI 91,8/100, EGDI 95,3/100, GCI 100,0/100, AI readiness 69,5/100. La dimensione più robusta è maturità infrastrutturale (9,7/10), mentre la criticità relativa riguarda indipendenza della supply chain (7,1/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Emirati Arabi Uniti è 9,7/10. La base statistica rileva utenti Internet pari al 100,0% nel 2024; 40,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 4.192 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Emirati Arabi Uniti al posto 19 con un valore medio di 69,5/100; il pilastro migliore è adozione pubblica (97,3/100), quello più debole è resilienza (43,1/100). Il GTMI 2025 è 91,8/100. Il punteggio S2 è 7,7/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Emirati Arabi Uniti è valutata sufficiente ma disomogenea, con S3 pari a 7,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 94,4/100, sviluppo e diffusione dell'IA 57,3/100, penetrazione Internet 100,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Emirati Arabi Uniti ottiene S4 7,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Emirati Arabi Uniti, Mercato multi-fornitore con forte presenza statunitense, europea e cinese; crescente capacità sovrana e partnership nazionali. L'impatto sulla valutazione è misurato da S4=7,1/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Emirati Arabi Uniti è S5 7,8/10. La base ITU registra ITU GCI 100,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure giuridiche (20,0/20). Freedom on the Net è 28/100 - Non libero, mentre Freedom in the World è Non libero (18/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Federal Decree-Law 45/2021 sulla protezione dei dati, regimi DIFC/ADGM e normative cyber federali; molteplicità di giurisdizioni e accessi pubblici da mappare.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	8,0	Crimini finanziari	9,0
Reti criminali	6,5	Attori incorporati nello Stato	6,5
Attori stranieri	7,0	Attori del settore privato	7,5
Resilienza complessiva	5,1	Cooperazione internazionale	5,0
Politiche e norme nazionali	5,5	Forze dell'ordine	6,0
Antiriciclaggio	3,5	Prevenzione	6,5
Supporto vittime e testimoni	6,0	Rischio operativo FOTR-CY	7,0 - ALTO

Sintesi del rischio cybercrime. Emirati Arabi Uniti presenta un'esposizione stimata alta (7,0/10): reati cyber-dipendenti 8,0/10, crimini finanziari 9,0/10 e resilienza 5,1/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori del settore privato (7,5/10) e attori stranieri (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Emirati Arabi Uniti assumono particolare rilevanza phishing e credential theft, ransomware, frodi d'investimento, attacchi a energia e servizi pubblici, abuso di cripto-attività e campagne che possono combinare profitto, spionaggio e pressione politica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Emirati Arabi Uniti, la resilienza complessiva è debole (5,1/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è intermedia (6,0/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 6,5/10 e supporto a vittime e testimoni 6,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Emirati Arabi Uniti, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Emirati Arabi Uniti. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Emirati Arabi Uniti, In Emirati Arabi Uniti le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Emirati Arabi Uniti, Il livello governativo di Emirati Arabi Uniti presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Emirati Arabi Uniti, Sul piano militare e dual-use, Emirati Arabi Uniti mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Emirati Arabi Uniti, Federal Decree-Law 45/2021 sulla protezione dei dati, regimi DIFC/ADGM e normative cyber federali; molteplicità di giurisdizioni e accessi pubblici da mappare. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Emirati Arabi Uniti, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 6,5/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,7	7,7	7,8	7,1	7,8	8,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
7,4	8,5	6,4	6,6	7,8	6,5

Il GCRI di Emirati Arabi Uniti è 8,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 7,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (8,5/10), mentre il più basso è Trasparenza istituzionale (6,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio

La matrice applica il FOTR di 7,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Emirati Arabi Uniti, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Emirati Arabi Uniti, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Emirati Arabi Uniti, Dal punto di vista italiano, Emirati Arabi Uniti rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale,

trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Emirati Arabi Uniti è favorevole ma condizionata: il valore FOTR di 7,2/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Trasparenza istituzionale.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

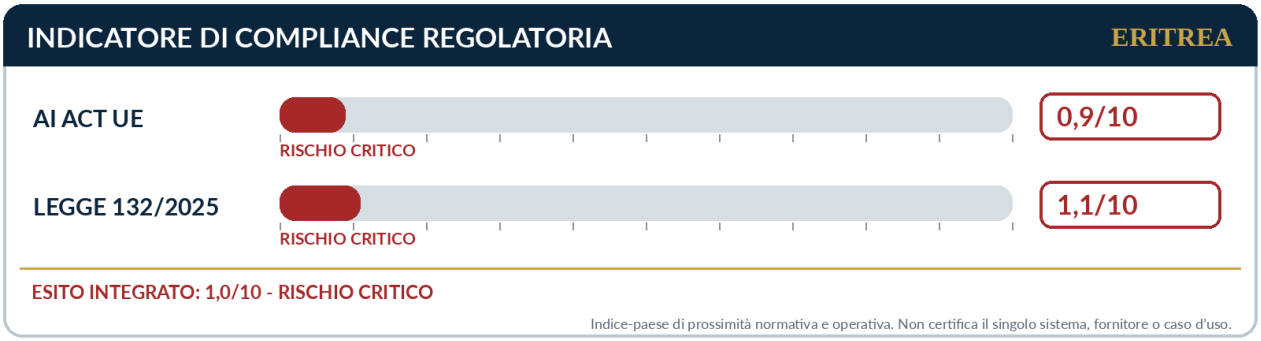
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Emirati Arabi Uniti: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Eritrea

Posizione FOTR	202	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	1,0	GCRI / 10	1,6	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Eritrea, AI Act UE 0,9/10; legge 132/2025 1,1/10; esito integrato 1,0/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Per un operatore italiano, Eritrea non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 3/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (1,6/10) e indice FOTR (1,0/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il rapporto digitale con Eritrea deve essere considerato eccezionale e ad alta esposizione. Sono necessari screening sanzionatori, autorizzazioni, segregazione completa e impossibilità tecnica di accedere ai dati in chiaro.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	14,3% / 0,2 per 100	2020/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	55,3% / 2 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	15,8 / 2,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	2,2/100 - Tier 5 - capacità iniziali	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	10,3/100 - rank 193	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (3/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	1,5 / 2,2 / 4,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Eritrea, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Eritrea le evidenze principali sono GTMI 2,7/100, EGDI 15,8/100, GCI 2,2/100, AI readiness 10,3/100. La dimensione più robusta è indipendenza della supply chain (3,3/10), mentre la criticità relativa riguarda postura di sicurezza cyber (0,4/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Eritrea è 1,6/10. La base statistica rileva utenti Internet pari al 14,3% nel 2020; 0,2 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 55,3% nel 2024; 2 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Eritrea al posto 193 con un valore medio di 10,3/100; il pilastro migliore è infrastrutture IA (25,4/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 2,7/100. Il punteggio S2 è 0,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Eritrea è valutata fragile, con S3 pari a 2,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 33,2/100, sviluppo e diffusione dell'IA 16,0/100, penetrazione Internet 14,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Eritrea ottiene S4 3,3/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Eritrea, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=3,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Eritrea è S5 0,4/10. La base ITU registra ITU GCI 2,2/100, Tier 5 - capacità iniziali; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (3/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Assenza di un quadro trasparente e indipendente di protezione dei dati; controllo statale delle comunicazioni e connettività limitata.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	1,5	Crimini finanziari	4,0
Reti criminali	5,0	Attori incorporati nello Stato	9,5
Attori stranieri	2,5	Attori del settore privato	1,5
Resilienza complessiva	2,2	Cooperazione internazionale	2,0
Politiche e norme nazionali	2,5	Forze dell'ordine	2,5
Antiriciclaggio	3,0	Prevenzione	1,5
Supporto vittime e testimoni	1,0	Rischio operativo FOTR-CY	4,9 - MODERATO

Pressione del crimine digitale. Il profilo di Eritrea restituisce un rischio FOTR-CY di 4,9/10 (moderato). La componente cyber-dipendente vale 1,5/10 e quella finanziaria 4,0/10; la risposta sistemica è valutata molto debole, con resilienza media di 2,2/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,5/10) e reti criminali (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Eritrea assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Eritrea, la resilienza complessiva è molto debole (2,2/10); la cooperazione internazionale è molto debole (2,0/10), le politiche e norme nazionali sono molto deboli (2,5/10) e la capacità delle forze dell'ordine è molto debole (2,5/10). Completano il quadro antiriciclaggio 3,0/10, prevenzione 1,5/10 e supporto a vittime e testimoni 1,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Eritrea, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Eritrea. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Eritrea, In Eritrea le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Eritrea, Il livello governativo di Eritrea presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Eritrea, Sul piano militare e dual-use, Eritrea mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Eritrea, Assenza di un quadro trasparente e indipendente di protezione dei dati; controllo statale delle comunicazioni e connettività limitata. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Eritrea, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 0,0/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
1,6	0,9	2,0	3,3	0,4	1,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
1,4	1,2	0,0	2,1	1,5	0,0

Il GCRI di Eritrea è 1,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 1,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (2,1/10), mentre il più basso è Trasparenza istituzionale (0,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 1,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Eritrea, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Eritrea, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Eritrea, Dal punto di vista italiano, Eritrea rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Eritrea, il FOTR di 1,0/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.
Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

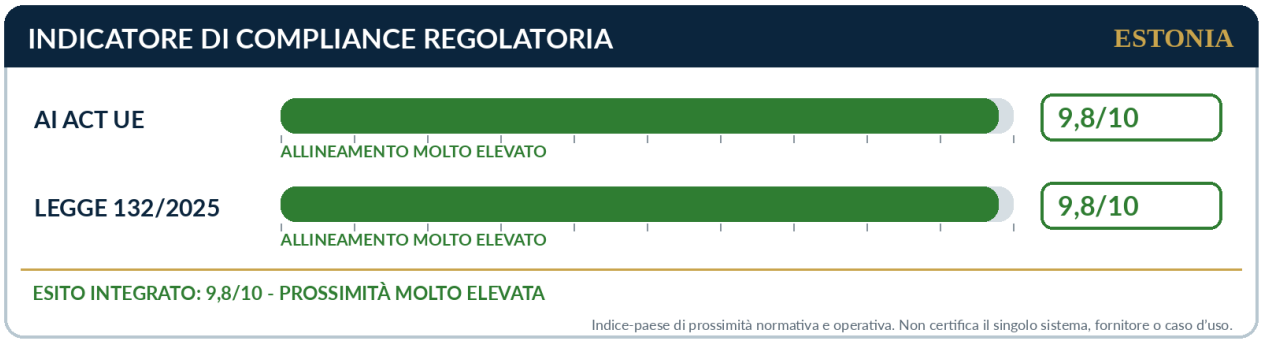
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Eritrea: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Estonia

Posizione FOTR	3	**Area**	Europa	**Subregione**	Europa settentrionale e baltica
Status	Stato membro delle Nazioni Unite	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	7/7 famiglie
FOTR / 10	**9,4**	**GCRI / 10**	**8,3**	**Classe operativa**	**Affidabilità molto alta**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Estonia, AI Act UE 9,8/10; legge 132/2025 9,8/10; esito integrato 9,8/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Estonia è stato membro delle nazioni unite collocato in Europa settentrionale e baltica. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 96/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (9,4/10) supera il GCRI tecnico (8,3/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Estonia presenta un ecosistema digitale maturo, istituzioni generalmente prevedibili e una buona capacità di gestione degli incidenti. Il rischio residuo deriva soprattutto dalla concentrazione cloud, dalle dipendenze extraeuropee e dalla complessità delle filiere software.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	92,2% / 35,4 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 139.022 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	97,3 / 99,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	95,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	75,1/100 - rank 21	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	91/100 - Libero / Libero (96/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,0 / 8,0 / 4,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Estonia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Estonia le evidenze principali sono GTMI 99,0/100, EGDI 97,3/100, GCI 95,0/100, AI readiness 75,1/100. La dimensione più robusta è maturità infrastrutturale (9,5/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,5/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Estonia è 9,5/10. La base statistica rileva utenti Internet pari al 92,2% nel 2024; 35,4 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 139.022 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Estonia al posto 21 con un valore medio di 75,1/100; il pilastro migliore è adozione pubblica (99,6/100), quello più debole è sviluppo e diffusione (46,0/100). Il GTMI 2025 è 99,0/100. Il punteggio S2 è 8,1/10 e indica una capacità elevata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Estonia è valutata solida, con S3 pari a 8,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 95,0/100, sviluppo e diffusione dell'IA 46,0/100, penetrazione Internet 92,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Estonia ottiene S4 6,5/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Estonia, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,5/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Estonia è S5 9,3/10. La base ITU registra ITU GCI 95,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure tecniche (15,3/20). Freedom on the Net è 91/100 - Libero, mentre Freedom in the World è Libero (96/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, Personal Data Protection Act, Cybersecurity Act nazionale e normativa UE; forte integrazione con identità digitale ed e-government.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,0	Crimini finanziari	7,0
Reti criminali	3,5	Attori incorporati nello Stato	2,0
Attori stranieri	5,5	Attori del settore privato	5,0
Resilienza complessiva	8,0	Cooperazione internazionale	8,5
Politiche e norme nazionali	8,0	Forze dell'ordine	7,5
Antiriciclaggio	8,0	Prevenzione	8,5
Supporto vittime e testimoni	7,5	Rischio operativo FOTR-CY	4,7 - MODERATO

Sintesi del rischio cybercrime. Estonia presenta un'esposizione stimata moderata (4,7/10): reati cyber-dipendenti 7,0/10, crimini finanziari 7,0/10 e resilienza 8,0/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (5,5/10) e attori del settore privato (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Estonia assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Estonia, la resilienza complessiva è robusta (8,0/10); la cooperazione internazionale è robusta (8,5/10), le politiche e norme nazionali sono robuste (8,0/10) e la capacità delle forze dell'ordine è robusta (7,5/10). Completano il quadro antiriciclaggio 8,0/10, prevenzione 8,5/10 e supporto a vittime e testimoni 7,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Estonia, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Estonia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Estonia, In Estonia le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Estonia, Il livello governativo di Estonia presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. L'affidabilità deve

essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Estonia, Sul piano militare e dual-use, Estonia mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Estonia, GDPR, Personal Data Protection Act, Cybersecurity Act nazionale e normativa UE; forte integrazione con identità digitale ed e-government. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Estonia, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 10,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,5	8,1	8,2	6,5	9,3	8,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
10,0	8,9	9,1	10,0	8,3	10,0

Il GCRI di Estonia è 8,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 9,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (10,0/10), mentre il più basso è Supply chain (8,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Basso	Basso	Basso

La matrice applica il FOTR di 9,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Estonia, la matrice non individua ambiti ad alto rischio; 6 categorie risultano basse o medio-basse, ferma la verifica del singolo progetto. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Estonia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Estonia, Dal punto di vista italiano, Estonia rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Estonia, il FOTR di 9,4/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (8,3/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

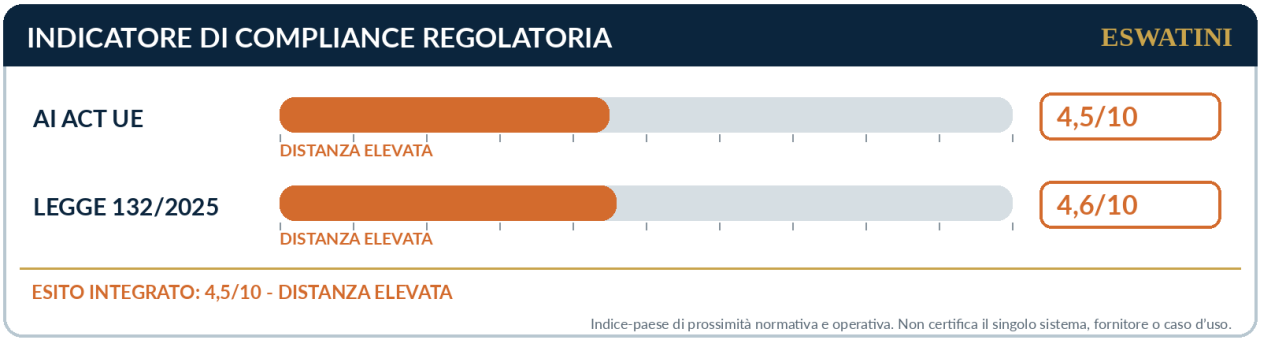
Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Estonia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Eswatini

Posizione FOTR	138	Area	Africa	Subregione	Africa australe
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,6	GCRI / 10	5,0	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Eswatini, AI Act UE 4,5/10; legge 132/2025 4,6/10; esito integrato 4,5/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Eswatini presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 17/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,0/10) e indice FOTR (4,6/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Eswatini è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	63,4% / 2,5 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	89,3% / 117 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	60,8 / 45,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	79,4/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	28,2/100 - rank 137	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (17/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 3,2 / 5,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Eswatini, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Eswatini le evidenze principali sono GTMI 45,9/100, EGDI 60,8/100, GCI 79,4/100, AI readiness 28,2/100. La dimensione più robusta è postura di sicurezza cyber (6,7/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,5/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Eswatini è 5,9/10. La base statistica rileva utenti Internet pari al 63,4% nel 2024; 2,5 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 89,3% nel 2024; 117 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Eswatini al posto 137 con un valore medio di 28,2/100; il pilastro migliore è governance (43,0/100), quello più debole è sviluppo e diffusione (10,6/100). Il GTMI 2025 è 45,9/100. Il punteggio S2 è 3,5/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Eswatini è valutata fragile, con S3 pari a 4,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 58,4/100, sviluppo e diffusione dell'IA 10,6/100, penetrazione Internet 63,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Eswatini ottiene S4 4,9/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Eswatini, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,9/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Eswatini è S5 6,7/10. La base ITU registra ITU GCI 79,4/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (10,2/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (17/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	6,0
Reti criminali	5,5	Attori incorporati nello Stato	6,5
Attori stranieri	4,5	Attori del settore privato	6,0
Resilienza complessiva	3,2	Cooperazione internazionale	5,0
Politiche e norme nazionali	3,0	Forze dell'ordine	3,0
Antiriciclaggio	4,5	Prevenzione	4,0
Supporto vittime e testimoni	2,5	Rischio operativo FOTR-CY	5,7 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Eswatini presenta un'esposizione stimata significativa (5,7/10): reati cyber-dipendenti 5,0/10, crimini finanziari 6,0/10 e resilienza 3,2/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (6,5/10) e attori del settore privato (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Eswatini assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Eswatini, la resilienza complessiva è molto debole (3,2/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono molto deboli (3,0/10) e la capacità delle forze dell'ordine è molto debole (3,0/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 4,0/10 e supporto a vittime e testimoni 2,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Eswatini, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Eswatini. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Eswatini, In Eswatini le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità

del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Eswatini, Il livello governativo di Eswatini presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Eswatini, Sul piano militare e dual-use, Eswatini mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Eswatini, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Eswatini, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,5/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
5,9	3,5	4,2	4,9	6,7	5,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,7	4,4	4,4	5,0	4,4	4,5

Il GCRI di Eswatini è 5,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,0/10), mentre il più basso è Maturità cyber (4,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Eswatini, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Eswatini, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Eswatini, Dal punto di vista italiano, Eswatini rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Eswatini ricade nella fascia di alto rischio (4,6/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

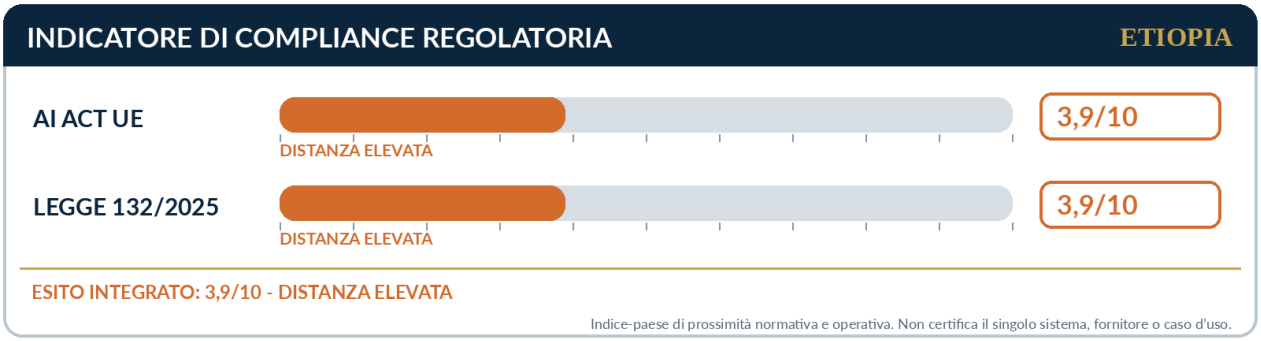
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Eswatini: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Etiopia

Posizione FOTR	179	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	3,8	GCRI / 10	4,2	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Etiopia, AI Act UE 3,9/10; legge 132/2025 3,9/10; esito integrato 3,9/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Etiopia, situato in Africa orientale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La partecipazione al coordinamento BRICS segnala una strategia di autonomia e diversificazione rispetto agli ecosistemi occidentali, con relazioni tecnologiche più intense verso Cina, Russia o altri poli emergenti. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 18/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (4,2/10) e indice FOTR (3,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il contesto di Etiopia richiede una presunzione prudenziale sfavorevole: anche contratti formalmente corretti possono non compensare carenze nei rimedi, nella continuità o nel controllo della supply chain.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	21,9% / 0,6 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	56,6% / 24 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	31,1 / 64,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	76,3/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	44,2/100 - rank 91	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	30/100 - Non libero / Non libero (18/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 4,5 / 6,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Etiopia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Etiopia le evidenze principali sono GTMI 64,3/100, EGDI 31,1/100, GCI 76,3/100, AI readiness 44,2/100. La dimensione più robusta è postura di sicurezza cyber (5,5/10), mentre la criticità relativa riguarda maturità infrastrutturale (2,5/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Etiopia è 2,5/10. La base statistica rileva utenti Internet pari al 21,9% nel 2024; 0,6 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 56,6% nel 2024; 24 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Etiopia al posto 91 con un valore medio di 44,2/100; il pilastro migliore è governance (54,9/100), quello più debole è infrastrutture IA (28,4/100). Il GTMI 2025 è 64,3/100. Il punteggio S2 è 4,5/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Etiopia è valutata fragile, con S3 pari a 3,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 32,5/100, sviluppo e diffusione dell'IA 38,7/100, penetrazione Internet 21,9%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Etiopia ottiene S4 4,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Etiopia, Forte presenza cinese nelle telecomunicazioni e nelle infrastrutture, con crescente ingresso di altri operatori. L'impatto sulla valutazione è misurato da S4=4,6/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Etiopia è S5 5,5/10. La base ITU registra ITU GCI 76,3/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è organizzazione (12,1/20). Freedom on the Net è 30/100 - Non libero, mentre Freedom in the World è Non libero (18/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Proclamazioni su telecomunicazioni, reati informatici e dati in evoluzione; liberalizzazione parziale e forte ruolo statale.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	7,0
Reti criminali	7,0	Attori incorporati nello Stato	6,0
Attori stranieri	6,0	Attori del settore privato	6,5
Resilienza complessiva	4,5	Cooperazione internazionale	5,5
Politiche e norme nazionali	6,0	Forze dell'ordine	4,0
Antiriciclaggio	6,0	Prevenzione	5,0
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	6,2 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Etiopia restituisce un rischio FOTR-CY di 6,2/10 (significativo). La componente cyber-dipendente vale 5,5/10 e quella finanziaria 7,0/10; la risposta sistemica è valutata debole, con resilienza media di 4,5/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (7,0/10) e attori del settore privato (6,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Etiopia assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Etiopia, la resilienza complessiva è debole (4,5/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 5,0/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Etiopia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Etiopia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Etiopia, In Etiopia le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Etiopia, Il livello governativo di Etiopia presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Etiopia, Sul piano militare e dual-use, Etiopia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Etiopia, Proclamazioni su telecomunicazioni, reati informatici e dati in evoluzione; liberalizzazione parziale e forte ruolo statale. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Etiopia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 3,8/10 e il rischio sui dati personali è Alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
2,5	4,5	3,8	4,6	5,5	4,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
3,7	3,9	3,6	4,4	3,6	3,8

Il GCRI di Etiopia è 4,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 3,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (4,4/10), mentre il più basso è Trasparenza istituzionale (3,6/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Alto	Alto	Alto	Alto	Alto	Alto

La matrice applica il FOTR di 3,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Etiopia, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Etiopia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Etiopia, Dal punto di vista italiano, Etiopia rientra nella classe «Rischio alto»: cooperazione eccezionale e ad alto controllo, subordinata a assenza di dati sensibili, verifica sanzionatoria, autorizzazioni interne e impossibilità di accesso ai sistemi strategici. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Etiopia ricade nella fascia di alto rischio (3,8/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

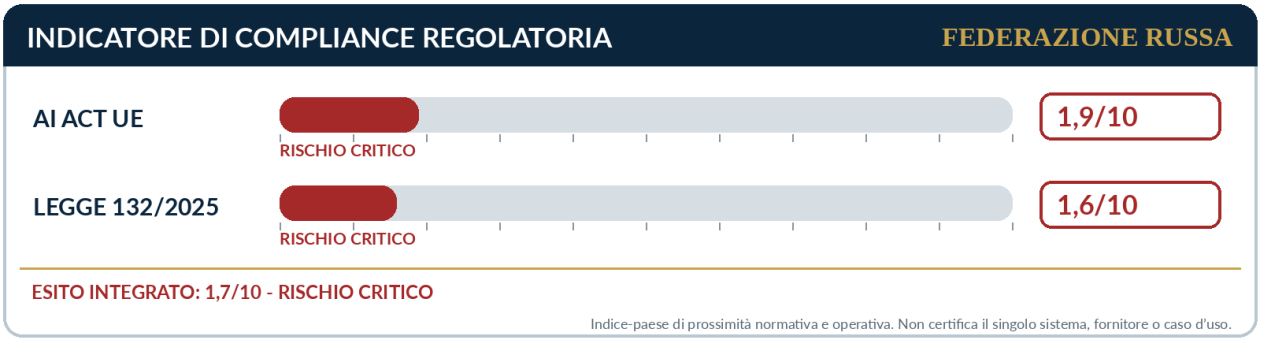
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Etiopia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Federazione Russa

Posizione FOTR	198	Area	Europa	Subregione	Europa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	1,3	GCRI / 10	6,3	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Federazione Russa, AI Act UE 1,9/10; legge 132/2025 1,6/10; esito integrato 1,7/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

La Federazione Russa dispone di capacità informatiche, spaziali, militari e di influenza digitale avanzate, ma il quadro geopolitico, sanzionatorio e di sicurezza rende la cooperazione tecnologica con soggetti italiani altamente critica. Le competenze tecniche e la presenza di fornitori nazionali non compensano i rischi connessi a controllo statale, opacità, conflitto, restrizioni sui dati e possibili impieghi dual-use. La valutazione dell'Atlante deve essere applicata insieme a sanzioni, controllo delle esportazioni e determinazioni delle autorità di sicurezza. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 12/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (6,3/10) è superiore al punteggio FOTR (1,3/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Capacità tecnologiche e cyber rilevanti, ma quadro sanzionatorio, accessi pubblici, conflitto geopolitico e limitazioni ai rimedi rendono il rapporto altamente critico per soggetti italiani.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	94,4% / 27,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 26.105 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	85,3 / 96,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	92,1/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	60,6/100 - rank 49	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	17/100 - Non libero / Non libero (12/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	9,0 / 3,4 / 7,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Federazione Russa, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Federazione Russa le evidenze principali sono GTMI 96,0/100, EGDI 85,3/100, GCI 92,1/100, AI readiness 60,6/100. La dimensione più robusta è maturità infrastrutturale (8,5/10), mentre la criticità relativa riguarda postura di sicurezza cyber (4,8/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Federazione Russa è 8,5/10. La base statistica rileva utenti Internet pari al 94,4% nel 2024; 27,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 26.105 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Federazione Russa al posto 49 con un valore medio di 60,6/100; il pilastro migliore è governance (74,1/100), quello più debole è resilienza (47,1/100). Il GTMI 2025 è 96,0/100. Il punteggio S2 è 6,9/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Federazione Russa è valutata sufficiente ma disomogenea, con S3 pari a 6,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 83,2/100, sviluppo e diffusione dell'IA 49,6/100, penetrazione Internet 94,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Federazione Russa ottiene S4 5,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina, Russia; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Federazione Russa, Fornitura domestica e russa, con crescente ricorso a ecosistemi cinesi e a canali indiretti per componenti soggetti a restrizioni. L'impatto sulla valutazione è misurato da S4=5,3/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Federazione Russa è S5 4,8/10. La base ITU registra ITU GCI 92,1/100, Tier 2 - avanzato; il pilastro relativamente più debole è misure tecniche (16,6/20). Freedom on the Net è 17/100 - Non libero, mentre Freedom in the World è Non libero (12/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Legge federale 152-FZ, localizzazione dei dati, Sovereign Internet e ampi poteri di sicurezza; sanzioni, accessi pubblici e limitazioni ai rimedi determinano criticità estreme.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	9,0	Crimini finanziari	8,5
Reti criminali	7,0	Attori incorporati nello Stato	9,0
Attori stranieri	5,0	Attori del settore privato	8,0
Resilienza complessiva	3,4	Cooperazione internazionale	3,0
Politiche e norme nazionali	5,5	Forze dell'ordine	4,0
Antiriciclaggio	3,5	Prevenzione	3,0
Supporto vittime e testimoni	2,5	Rischio operativo FOTR-CY	7,9 - ALTO

Quadro criminale digitale. Per Federazione Russa, l'indice operativo FOTR-CY è 7,9/10, classe alta. Il mercato dei reati cyber-dipendenti è molto elevato (9,0/10), mentre i crimini finanziari sono molto elevati (8,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e attori del settore privato (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Federazione Russa assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Federazione Russa, la resilienza complessiva è molto debole (3,4/10); la cooperazione internazionale è molto debole (3,0/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 3,0/10 e supporto a vittime e testimoni 2,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Federazione Russa, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; blocco di hosting e ASN ad alta reputazione negativa, ricerca proattiva delle minacce su malware sottrattori di informazioni e controllo dei canali RDP/VPN; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Federazione Russa. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Federazione Russa, In Federazione Russa le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Federazione Russa, Il livello governativo di Federazione Russa presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Federazione Russa, Sul piano militare e dual-use, Federazione Russa mostra forte integrazione o dipendenza dall'ecosistema russo, inclusi sistemi di comando, comunicazione e sicurezza. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Federazione Russa, Legge federale 152-FZ, localizzazione dei dati, Sovereign Internet e ampi poteri di sicurezza; sanzioni, accessi pubblici e limitazioni ai rimedi determinano criticità estreme. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Federazione Russa, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 0,0/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,5	6,9	6,2	5,3	4,8	6,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
1,8	2,9	0,6	0,3	2,0	0,0

Il GCRI di Federazione Russa è 6,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 1,3/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (2,9/10), mentre il più basso è Trasferibilità dati (0,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 1,3/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Federazione Russa, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Federazione Russa, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Federazione Russa, Dal punto di vista italiano, Federazione Russa rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il

punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Federazione Russa, il FOTR di 1,3/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

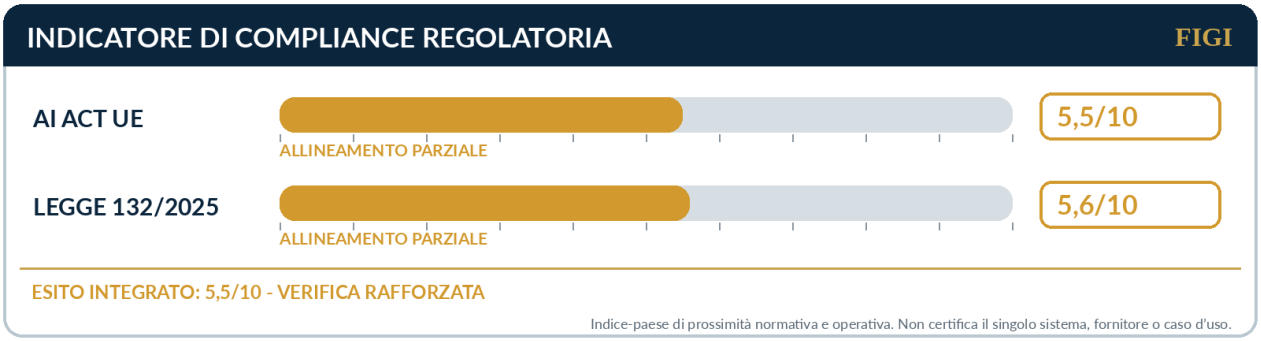
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Federazione Russa: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Figi

Posizione FOTR	108	Area	Oceania	Subregione	Pacifico insulare
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,6	GCRI / 10	5,1	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Figi, AI Act UE 5,5/10; legge 132/2025 5,6/10; esito integrato 5,5/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Figi è stato membro delle nazioni unite collocato in Pacifico insulare. La distanza geografica e l'insularità rendono centrali cavi sottomarini, satelliti, continuità energetica e dipendenza da fornitori australiani, neozelandesi, statunitensi o asiatici. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 72/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,1/10) e indice FOTR (5,6/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. In Figi la trasformazione digitale procede più rapidamente dell'uniformità regolatoria e operativa. Gli investimenti devono essere accompagnati da audit, clausole di uscita e gestione locale del rischio.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	74,7% / 1,8 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	95,9% / 222 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	67,5 / 56,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	53,8/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	37,0/100 - rank 108	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (72/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 5,4 / 4,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Figi, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Figi le evidenze principali sono GTMI 56,3/100, EGDI 67,5/100, GCI 53,8/100, AI readiness 37,0/100. La dimensione più robusta è maturità infrastrutturale (6,1/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,3/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Figi è 6,1/10. La base statistica rileva utenti Internet pari al 74,7% nel 2024; 1,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 95,9% nel 2024; 222 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Figi al posto 108 con un valore medio di 37,0/100; il pilastro migliore è adozione pubblica (65,9/100), quello più debole è politiche pubbliche (15,5/100). Il GTMI 2025 è 56,3/100. Il punteggio S2 è 4,3/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Figi è valutata sufficiente ma disomogenea, con S3 pari a 5,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 74,1/100, sviluppo e diffusione dell'IA 31,2/100, penetrazione Internet 74,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Figi ottiene S4 4,3/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Figi, Dipendenza da Australia, Nuova Zelanda, Stati Uniti, Francia e operatori satellitari o sottomarini; la scala ridotta limita la diversificazione e aumenta il rischio di concentrazione. L'impatto sulla

valutazione è misurato da S4=4,3/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Figi è S5 5,4/10. La base ITU registra ITU GCI 53,8/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (1,4/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (72/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	5,5
Reti criminali	5,5	Attori incorporati nello Stato	4,0
Attori stranieri	6,0	Attori del settore privato	3,0
Resilienza complessiva	5,4	Cooperazione internazionale	5,5
Politiche e norme nazionali	6,0	Forze dell'ordine	5,0
Antiriciclaggio	6,0	Prevenzione	5,5
Supporto vittime e testimoni	5,5	Rischio operativo FOTR-CY	4,9 - MODERATO

Pressione del crimine digitale. Il profilo di Figi restituisce un rischio FOTR-CY di 4,9/10 (moderato). La componente cyber-dipendente vale 4,5/10 e quella finanziaria 5,5/10; la risposta sistemica è valutata debole, con resilienza media di 5,4/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (6,0/10) e reti criminali (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Figi assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Figi, la resilienza complessiva è debole (5,4/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 5,5/10 e supporto a vittime e testimoni 5,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Figi, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Figi. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Figi, In Figi le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Figi, Il livello governativo di Figi presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Figi, Sul piano militare e dual-use, Figi mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Figi, Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Figi, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,5/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,1	4,3	5,5	4,3	5,4	5,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,6	5,2	5,9	6,4	4,7	5,5

Il GCRI di Figi è 5,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,4/10), mentre il più basso è Supply chain (4,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio-alto	Medio-alto	Medio	Medio

La matrice applica il FOTR di 5,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Figi, 2 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Cloud e infrastrutture, IP e R&S. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Figi, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Figi, Dal punto di vista italiano, Figi rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Figi è indicata una cooperazione selettiva, coerente con il FOTR di 5,6/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Cloud e infrastrutture a decisione caso per caso.

Presidi minimi raccomandati

- Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
- Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
- Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
- Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

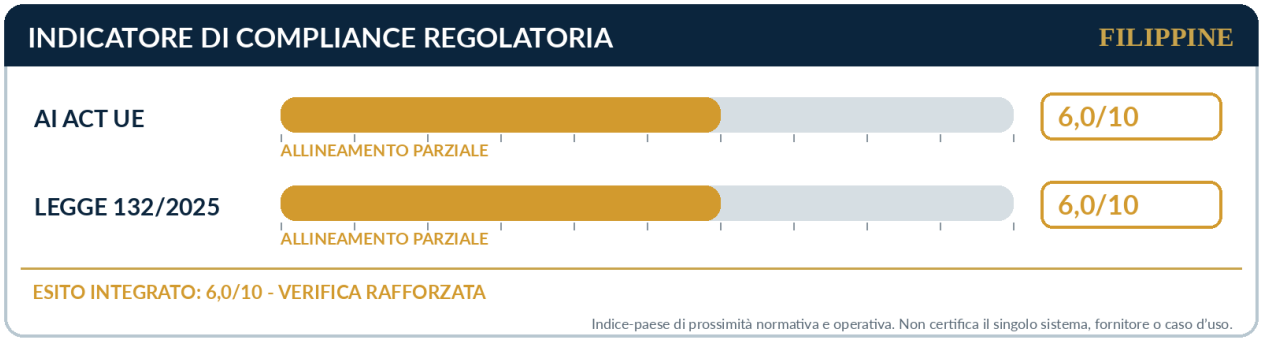
Profilo Celeborn Intelligence di Figi: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom

House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Filippine

Posizione FOTR	74	Area	Asia	Subregione	Asia sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	6,0	GCRI / 10	6,5	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Filippine, AI Act UE 6,0/10; legge 132/2025 6,0/10; esito integrato 6,0/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Asia, Filippine presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 58/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,5/10) e indice FOTR (6,0/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il quadro di Filippine è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	67,3% / 7,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	94,8% / 132 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	76,2 / 71,5	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	93,5/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	64,8/100 - rank 43	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	61/100 - Parzialmente libero / Parzialmente libero (58/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,5 / 4,5 / 7,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Filippine, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Filippine le evidenze principali sono GTMI 71,5/100, EGDI 76,2/100, GCI 93,5/100, AI readiness 64,8/100. La dimensione più robusta è postura di sicurezza cyber (7,7/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,6/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Filippine è 6,2/10. La base statistica rileva utenti Internet pari al 67,3% nel 2024; 7,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 94,8% nel 2024; 132 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Filippine al posto 43 con un valore medio di 64,8/100; il pilastro migliore è politiche pubbliche (84,5/100), quello più debole è sviluppo e diffusione (44,0/100). Il GTMI 2025 è 71,5/100. Il punteggio S2 è 6,6/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Filippine è valutata sufficiente ma disomogenea, con S3 pari a 6,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 72,6/100, sviluppo e diffusione dell'IA 44,0/100, penetrazione Internet 67,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Filippine ottiene S4 5,6/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Stati Uniti, Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Filippine, Prevalenza statunitense e asiatica, con operatori domestici e crescente presenza cinese in alcuni segmenti. L'impatto sulla valutazione è misurato da S4=5,6/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Filippine è S5 7,7/10. La base ITU registra ITU GCI 93,5/100, Tier 2 - avanzato; il pilastro relativamente più debole è sviluppo delle capacità (17,2/20). Freedom on the Net è 61/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (58/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Data Privacy Act 2012, National Privacy Commission e Cybercrime Prevention Act; quadro relativamente maturo, con capacità operativa disomogenea.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,5	Crimini finanziari	8,0
Reti criminali	6,5	Attori incorporati nello Stato	8,0
Attori stranieri	7,5	Attori del settore privato	3,5
Resilienza complessiva	4,5	Cooperazione internazionale	5,5
Politiche e norme nazionali	5,5	Forze dell'ordine	3,0
Antiriciclaggio	5,5	Prevenzione	4,5
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	7,0 - ALTO

Quadro criminale digitale. Per Filippine, l'indice operativo FOTR-CY è 7,0/10, classe alta. Il mercato dei reati cyber-dipendenti è molto elevato (7,5/10), mentre i crimini finanziari sono molto elevati (8,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e attori stranieri (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Filippine assumono particolare rilevanza centri organizzati di truffa, frodi d'investimento e sentimentali, phishing multicanale, batterie di schede SIM, conti prestanome, riciclaggio in cripto-attività e compromissione di servizi esternalizzati. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Filippine, la resilienza complessiva è debole (4,5/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è molto debole (3,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 4,5/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Filippine, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; controllo della filiera contro esposizione a complessi organizzati per truffe telematiche, call center coercitivi e conti prestanome; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Filippine. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Filippine, In Filippine le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Filippine, Il livello governativo di Filippine presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Filippine, Sul piano militare e dual-use, Filippine mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Filippine, Data Privacy Act 2012, National Privacy Commission e Cybercrime Prevention Act; quadro relativamente maturo, con capacità operativa disomogenea. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Filippine, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,6/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,2	6,6	6,5	5,6	7,7	6,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,2	6,6	5,4	5,8	6,3	5,6

Il GCRI di Filippine è 6,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Maturità cyber (6,6/10), mentre il più basso è Trasparenza istituzionale (5,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Filippine, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Filippine, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Filippine, Dal punto di vista italiano, Filippine rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Filippine è indicata una cooperazione selettiva, coerente con il FOTR di 6,0/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasparenza istituzionale a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

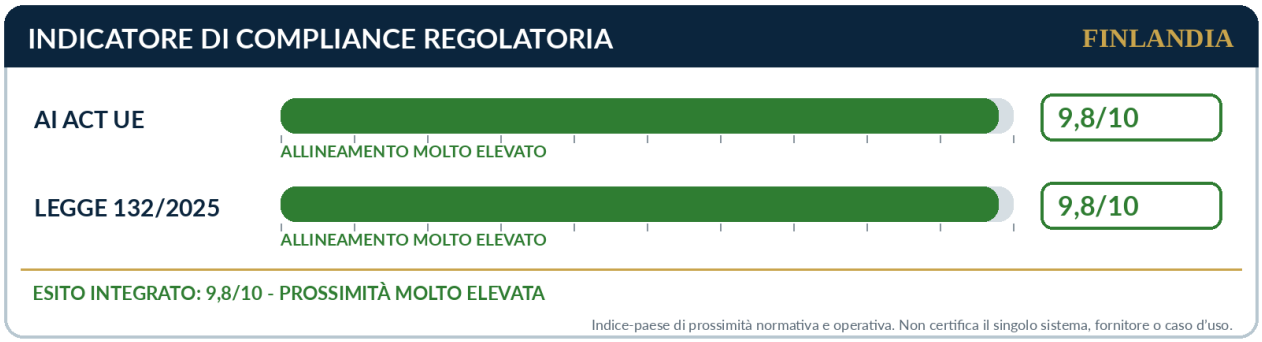
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Filippine: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Finlandia

Posizione FOTR	2	**Area**	Europa	**Subregione**	Europa settentrionale e baltica
Status	Stato membro delle Nazioni Unite	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	**9,5**	**GCRI / 10**	**8,4**	**Classe operativa**	**Affidabilità molto alta**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Finlandia, AI Act UE 9,8/10; legge 132/2025 9,8/10; esito integrato 9,8/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Finlandia, situato in Europa settentrionale e baltica, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 100/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (9,5/10) supera il GCRI tecnico (8,4/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Per un operatore italiano, Finlandia costituisce un ambiente digitale ad alta affidabilità: connettività, supervisione e continuità sono solide. La valutazione non deve però trascurare subfornitori, accessi transfrontalieri e tecnologie dual-use.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	93,7% / 36,5 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 177.934 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	95,7 / 83,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	100,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	72,2/100 - rank 18	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (100/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 8,4 / 3,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Finlandia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Finlandia le evidenze principali sono GTMI 83,7/100, EGDI 95,7/100, GCI 100,0/100, AI readiness 72,2/100. La dimensione più robusta è postura di sicurezza cyber (9,7/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,4/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Finlandia è 9,6/10. La base statistica rileva utenti Internet pari al 93,7% nel 2024; 36,5 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 177.934 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Finlandia al posto 18 con un valore medio di 72,2/100; il pilastro migliore è governance (84,2/100), quello più debole è infrastrutture IA (61,6/100). Il GTMI 2025 è 83,7/100. Il punteggio S2 è 7,6/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Finlandia è valutata solida, con S3 pari a 8,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 98,4/100, sviluppo e diffusione dell'IA 63,0/100, penetrazione Internet 93,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Finlandia ottiene S4 6,4/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open

source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Finlandia, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario, luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,4/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Finlandia è S5 9,7/10. La base ITU registra ITU GCI 100,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure giuridiche (20,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (100/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, Data Protection Act, Information Management Act e disciplina cyber/NIS2; applicazione diretta dei regolamenti digitali UE.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	4,5
Reti criminali	3,5	Attori incorporati nello Stato	1,5
Attori stranieri	4,0	Attori del settore privato	3,5
Resilienza complessiva	8,4	Cooperazione internazionale	9,0
Politiche e norme nazionali	8,5	Forze dell'ordine	8,5
Antiriciclaggio	8,0	Prevenzione	8,0
Supporto vittime e testimoni	8,0	Rischio operativo FOTR-CY	3,6 - MODERATO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (5,5/10), criminalità finanziaria (4,5/10) e resilienza (8,4/10) colloca Finlandia in una fascia di rischio moderato, pari a 3,6/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (4,0/10) e reti criminali (3,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Finlandia assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Finlandia, la resilienza complessiva è robusta (8,4/10); la cooperazione internazionale è robusta (9,0/10), le politiche e norme nazionali sono robuste (8,5/10) e la capacità delle forze dell'ordine è robusta (8,5/10). Completano il quadro antiriciclaggio 8,0/10, prevenzione 8,0/10 e supporto a vittime e testimoni 8,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Finlandia, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Finlandia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Finlandia, In Finlandia le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La

disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Finlandia, Il livello governativo di Finlandia presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Finlandia, Sul piano militare e dual-use, Finlandia mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Finlandia, GDPR, Data Protection Act, Information Management Act e disciplina cyber/NIS2; applicazione diretta dei regolamenti digitali UE. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Finlandia, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 10,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,6	7,6	8,6	6,4	9,7	8,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
10,0	9,4	8,7	10,0	8,7	10,0

Il GCRI di Finlandia è 8,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 9,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (10,0/10), mentre il più basso è Trasparenza istituzionale (8,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Basso	Basso	Basso

La matrice applica il FOTR di 9,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Finlandia, la matrice non individua ambiti ad alto rischio; 6 categorie risultano basse o medio-basse, ferma la verifica del singolo progetto. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Finlandia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Finlandia, Dal punto di vista italiano, Finlandia rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Finlandia, il FOTR di 9,5/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (8,7/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

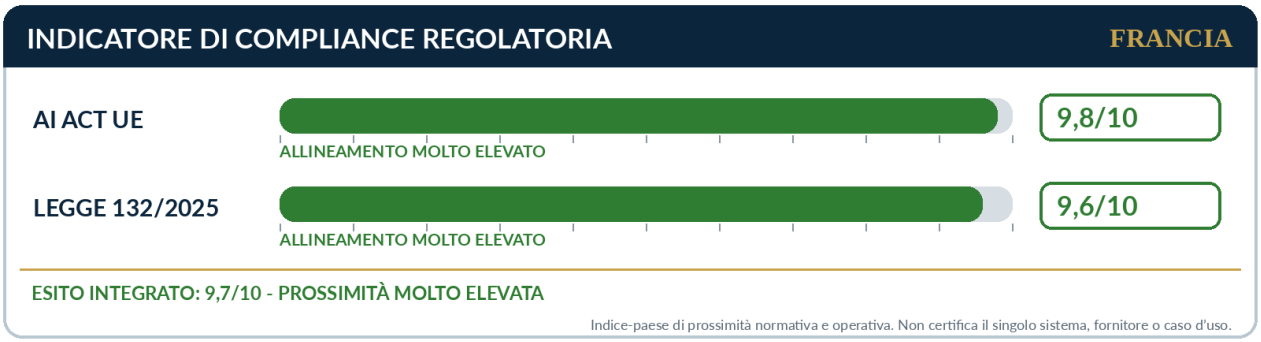
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Finlandia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Francia

Posizione FOTR	16	Area	Europa	Subregione	Europa occidentale e centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	8,9	GCRI / 10	8,6	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Francia, AI Act UE 9,8/10; legge 132/2025 9,6/10; esito integrato 9,7/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Per un operatore italiano, Francia non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 89/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,6/10) e indice FOTR (8,9/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il sistema digitale di Francia è avanzato e integrato con standard internazionali. Le principali criticità non sono di base istituzionale, ma riguardano supply chain, concentrazione dei servizi e gestione delle eccezioni di sicurezza nazionale.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	88,7% / 48,9 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 57.275 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	87,4 / 82,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	99,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	83,0/100 - rank 2	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	76/100 - Libero / Libero (89/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,5 / 7,0 / 5,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Francia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Francia le evidenze principali sono GTMI 82,4/100, EGDI 87,4/100, GCI 99,0/100, AI readiness 83,0/100. La dimensione più robusta è maturità infrastrutturale (9,4/10), mentre la criticità relativa riguarda indipendenza della supply chain (8,0/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Francia è 9,4/10. La base statistica rileva utenti Internet pari al 88,7% nel 2024; 48,9 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 57.275 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Francia al posto 2 con un valore medio di 83,0/100; il pilastro migliore è adozione pubblica (97,2/100), quello più debole è sviluppo e diffusione (68,2/100). Il GTMI 2025 è 82,4/100. Il punteggio S2 è 8,2/10 e indica una capacità elevata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Francia è valutata solida, con S3 pari a 8,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 85,6/100, sviluppo e diffusione dell'IA 68,2/100, penetrazione Internet 88,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Francia ottiene S4 8,0/10 e presenta buona capacità di diversificazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 8,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Francia, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=8,0/10 e dal proxy di indipendenza 8,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Francia è S5 9,0/10. La base ITU registra ITU GCI 99,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure tecniche (19,0/20). Freedom on the Net è 76/100 - Libero, mentre Freedom in the World è Libero (89/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, Loi Informatique et Libertés, Code de la défense e disciplina ANSSI; attuazione NIS2 e applicazione del corpus digitale UE.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,5	Crimini finanziari	6,5
Reti criminali	6,5	Attori incorporati nello Stato	3,5
Attori stranieri	7,5	Attori del settore privato	5,5
Resilienza complessiva	7,0	Cooperazione internazionale	8,5
Politiche e norme nazionali	7,5	Forze dell'ordine	7,0
Antiriciclaggio	8,0	Prevenzione	7,5
Supporto vittime e testimoni	6,0	Rischio operativo FOTR-CY	5,4 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (6,5/10), criminalità finanziaria (6,5/10) e resilienza (7,0/10) colloca Francia in una fascia di rischio significativo, pari a 5,4/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (7,5/10) e reti criminali (6,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Francia assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Francia, la resilienza complessiva è intermedia (7,0/10); la cooperazione internazionale è robusta (8,5/10), le politiche e norme nazionali sono robuste (7,5/10) e la capacità delle forze dell'ordine è intermedia (7,0/10). Completano il quadro antiriciclaggio 8,0/10, prevenzione 7,5/10 e supporto a vittime e testimoni 6,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Francia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Francia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Francia, In Francia le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Francia, Il livello governativo di Francia presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Francia, Sul piano militare e dual-use, Francia mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Francia, GDPR, Loi Informatique et Libertés, Code de la défense e disciplina ANSSI; attuazione NIS2 e applicazione del corpus digitale UE. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Francia, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,8/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,4	8,2	8,2	8,0	9,0	8,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,5	8,8	8,2	9,3	7,8	9,8

Il GCRI di Francia è 8,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,9/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,8/10), mentre il più basso è Supply chain (7,8/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Basso	Basso	Basso

La matrice applica il FOTR di 8,9/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Francia, la matrice non individua ambiti ad alto rischio; 6 categorie risultano basse o medio-basse, ferma la verifica del singolo progetto. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Francia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Francia, Dal punto di vista italiano, Francia rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Francia, il FOTR di 8,9/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (7,8/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

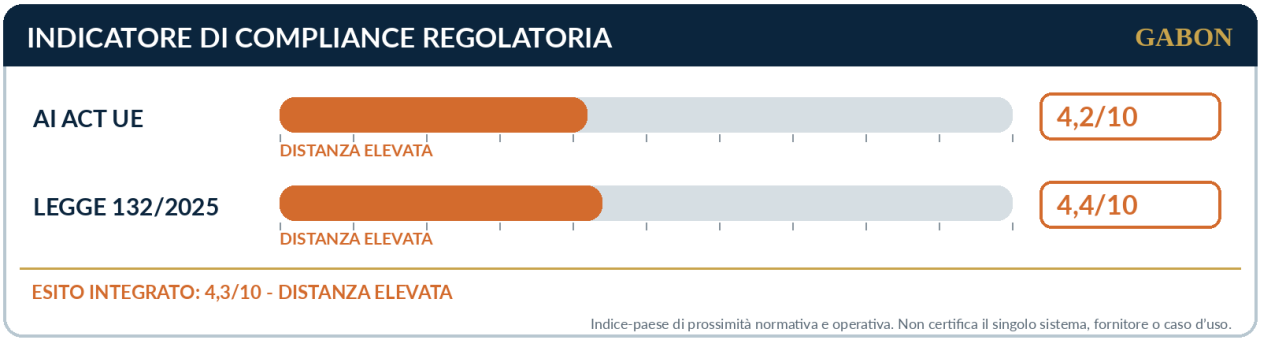
Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Francia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Gabon

Posizione FOTR	163	Area	Africa	Subregione	Africa centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,4	GCRI / 10	4,5	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Gabon, AI Act UE 4,2/10; legge 132/2025 4,4/10; esito integrato 4,3/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Gabon è stato membro delle nazioni unite collocato in Africa centrale. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 25/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (4,5/10) e indice FOTR (4,4/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per Gabon non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	68,7% / 4,7 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	95,1% / 87 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	57,4 / 25,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	39,9/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	27,8/100 - rank 133	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (25/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,5 / 3,5 / 5,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Gabon, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Gabon le evidenze principali sono GTMI 25,8/100, EGDI 57,4/100, GCI 39,9/100, AI readiness 27,8/100. La dimensione più robusta è maturità infrastrutturale (6,3/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Gabon è 6,3/10. La base statistica rileva utenti Internet pari al 68,7% nel 2024; 4,7 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 95,1% nel 2024; 87 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Gabon al posto 133 con un valore medio di 27,8/100; il pilastro migliore è governance (51,2/100), quello più debole è politiche pubbliche (16,0/100). Il GTMI 2025 è 25,8/100. Il punteggio S2 è 2,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Gabon è valutata fragile, con S3 pari a 4,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 57,7/100, sviluppo e diffusione dell'IA 20,4/100, penetrazione Internet 68,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Gabon ottiene S4 4,4/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Gabon, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,4/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Gabon è S5 4,1/10. La base ITU registra ITU GCI 39,9/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (25/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,5	Crimini finanziari	6,5
Reti criminali	4,5	Attori incorporati nello Stato	7,5
Attori stranieri	6,0	Attori del settore privato	5,5
Resilienza complessiva	3,5	Cooperazione internazionale	4,5
Politiche e norme nazionali	4,0	Forze dell'ordine	4,5
Antiriciclaggio	2,0	Prevenzione	3,5
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	5,2 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Gabon restituisce un rischio FOTR-CY di 5,2/10 (significativo). La componente cyber-dipendente vale 2,5/10 e quella finanziaria 6,5/10; la risposta sistemica è valutata debole, con resilienza media di 3,5/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,5/10) e attori stranieri (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Gabon assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Gabon, la resilienza complessiva è debole (3,5/10); la cooperazione internazionale è debole (4,5/10), le politiche e norme nazionali sono deboli (4,0/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 2,0/10, prevenzione 3,5/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Gabon, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Gabon. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Gabon, In Gabon le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità

del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Gabon, Il livello governativo di Gabon presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Gabon, Sul piano militare e dual-use, Gabon mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Gabon, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Gabon, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,1/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,3	2,9	4,6	4,4	4,1	4,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,4	4,4	4,3	5,0	3,9	4,1

Il GCRI di Gabon è 4,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,0/10), mentre il più basso è Supply chain (3,9/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Gabon, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Gabon, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Gabon, Dal punto di vista italiano, Gabon rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Gabon ricade nella fascia di alto rischio (4,4/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

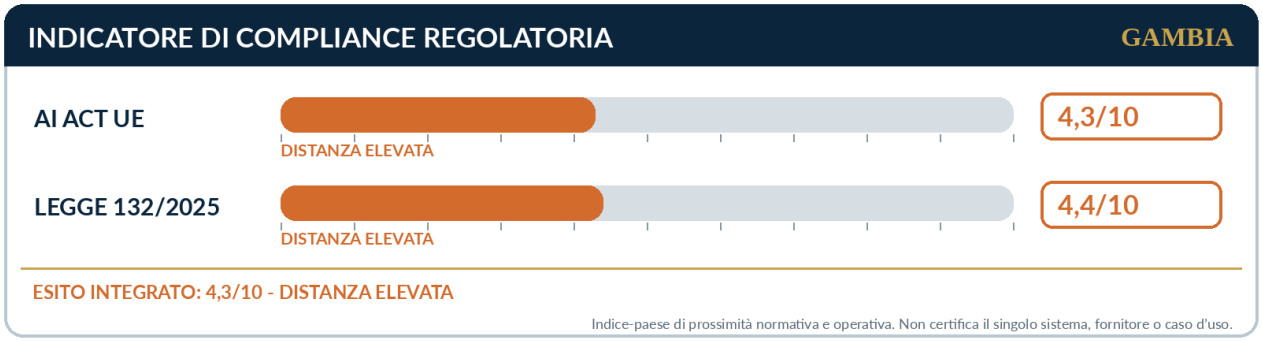
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Gabon: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Gambia

Posizione FOTR	146	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	4,5	GCRI / 10	3,8	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Gambia, AI Act UE 4,3/10; legge 132/2025 4,4/10; esito integrato 4,3/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Gambia presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 51/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (3,8/10) e indice FOTR (4,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Gambia è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	49,5% / 0,5 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	69,0% / 59 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	25,5 / 19,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	61,8/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	24,2/100 - rank 153	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	56/100 - Parzialmente libero / Parzialmente libero (51/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 5,1 / 4,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Gambia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Gambia le evidenze principali sono GTMI 19,9/100, EGDI 25,5/100, GCI 61,8/100, AI readiness 24,2/100. La dimensione più robusta è postura di sicurezza cyber (5,6/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,2/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Gambia è 3,8/10. La base statistica rileva utenti Internet pari al 49,5% nel 2024; 0,5 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 69,0% nel 2024; 59 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Gambia al posto 153 con un valore medio di 24,2/100; il pilastro migliore è governance (37,8/100), quello più debole è sviluppo e diffusione (10,3/100). Il GTMI 2025 è 19,9/100. Il punteggio S2 è 2,2/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Gambia è valutata fragile, con S3 pari a 2,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 28,2/100, sviluppo e diffusione dell'IA 10,3/100, penetrazione Internet 49,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Gambia ottiene S4 4,4/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Gambia, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,4/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Gambia è S5 5,6/10. La base ITU registra ITU GCI 61,8/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (8,8/20). Freedom on the Net è 56/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (51/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	6,0
Reti criminali	6,5	Attori incorporati nello Stato	7,0
Attori stranieri	5,0	Attori del settore privato	4,0
Resilienza complessiva	5,1	Cooperazione internazionale	5,5
Politiche e norme nazionali	5,5	Forze dell'ordine	5,0
Antiriciclaggio	5,0	Prevenzione	4,5
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	4,6 - MODERATO

Quadro criminale digitale. Per Gambia, l'indice operativo FOTR-CY è 4,6/10, classe moderata. Il mercato dei reati cyber-dipendenti è limitato o poco osservabile (2,0/10), mentre i crimini finanziari sono elevati (6,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,0/10) e reti criminali (6,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Gambia assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Gambia, la resilienza complessiva è debole (5,1/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 4,5/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Gambia, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Gambia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Gambia, In Gambia le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Gambia, Il livello governativo di Gambia presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Gambia, Sul piano militare e dual-use, Gambia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Gambia, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Gambia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,1/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,8	2,2	2,8	4,4	5,6	3,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,7	4,4	4,5	4,8	4,3	4,1

Il GCRI di Gambia è 3,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (4,8/10), mentre il più basso è Trasferibilità dati (4,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Gambia, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Gambia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Gambia, Dal punto di vista italiano, Gambia rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Gambia ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.
Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

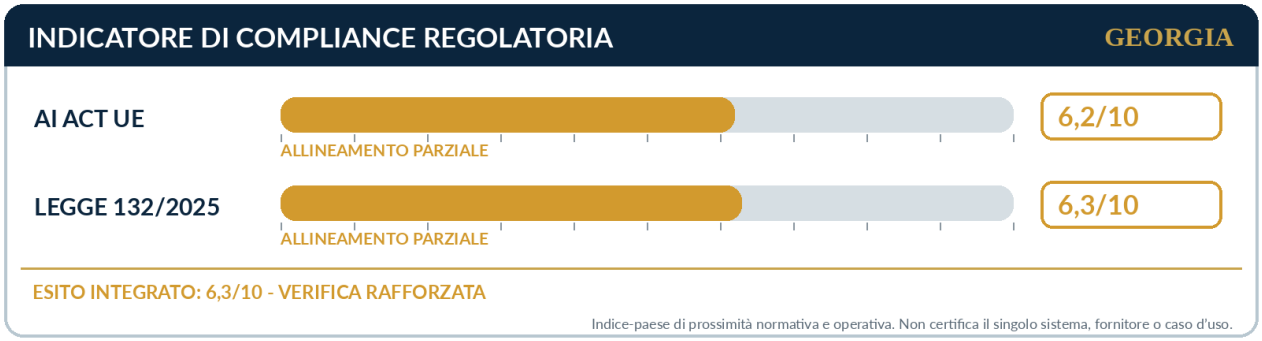
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Gambia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Georgia

Posizione FOTR	61	Area	Asia	Subregione	Caucaso meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	6,3	GCRI / 10	6,7	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Georgia, AI Act UE 6,2/10; legge 132/2025 6,3/10; esito integrato 6,3/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Georgia, situato in Caucaso meridionale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 51/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,7/10) e indice FOTR (6,3/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. In Georgia la trasformazione digitale procede più rapidamente dell'uniformità regolatoria e operativa. Gli investimenti devono essere accompagnati da audit, clausole di uscita e gestione locale del rischio.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	83,8% / 30,4 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 5.293 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	77,9 / 63,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	91,9/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	42,0/100 - rank 87	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	70/100 - Libero / Parzialmente libero (51/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 5,0 / 4,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Georgia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Georgia le evidenze principali sono GTMI 63,2/100, EGDI 77,9/100, GCI 91,9/100, AI readiness 42,0/100. La dimensione più robusta è maturità infrastrutturale (8,6/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,9/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Georgia è 8,6/10. La base statistica rileva utenti Internet pari al 83,8% nel 2024; 30,4 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 5.293 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Georgia al posto 87 con un valore medio di 42,0/100; il pilastro migliore è governance (74,2/100), quello più debole è politiche pubbliche (19,0/100). Il GTMI 2025 è 63,2/100. Il punteggio S2 è 4,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Georgia è valutata sufficiente ma disomogenea, con S3 pari a 6,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 86,5/100, sviluppo e diffusione dell'IA 27,2/100, penetrazione Internet 83,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Georgia ottiene S4 5,5/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Georgia, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo

societario e subfornitura. L'impatto sulla valutazione è misurato da S4=5,5/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Georgia è S5 8,0/10. La base ITU registra ITU GCI 91,9/100, Tier 2 - avanzato; il pilastro relativamente più debole è sviluppo delle capacità (16,3/20). Freedom on the Net è 70/100 - Libero, mentre Freedom in the World è Parzialmente libero (51/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge sulla protezione dei dati riformata e quadro cyber nazionale; progressiva convergenza europea con rischi geopolitici e di continuità.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	5,5
Reti criminali	3,5	Attori incorporati nello Stato	4,0
Attori stranieri	3,0	Attori del settore privato	5,5
Resilienza complessiva	5,0	Cooperazione internazionale	5,0
Politiche e norme nazionali	6,5	Forze dell'ordine	6,5
Antiriciclaggio	4,5	Prevenzione	5,5
Supporto vittime e testimoni	6,5	Rischio operativo FOTR-CY	4,6 - MODERATO

Pressione del crimine digitale. Il profilo di Georgia restituisce un rischio FOTR-CY di 4,6/10 (moderato). La componente cyber-dipendente vale 5,0/10 e quella finanziaria 5,5/10; la risposta sistemica è valutata debole, con resilienza media di 5,0/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori del settore privato (5,5/10) e attori incorporati nello Stato (4,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Georgia assumono particolare rilevanza ransomware come servizio, malware sottrattori di informazioni, infrastrutture di hosting permissive, DDoS, furto di credenziali, estorsione dei dati e possibili sovrapposizioni tra criminalità professionale e finalità geopolitiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Georgia, la resilienza complessiva è debole (5,0/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è intermedia (6,5/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 5,5/10 e supporto a vittime e testimoni 6,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Georgia, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; blocco di hosting e ASN ad alta reputazione negativa, ricerca proattiva delle minacce su malware sottrattori di informazioni e controllo dei canali RDP/VPN; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Georgia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Georgia, In Georgia le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Georgia, Il livello governativo di Georgia presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il

settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Georgia, Sul piano militare e dual-use, Georgia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Georgia, Legge sulla protezione dei dati riformata e quadro cyber nazionale; progressiva convergenza europea con rischi geopolitici e di continuità. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Georgia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,7/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,6	4,9	6,6	5,5	8,0	6,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,6	6,9	5,8	6,8	6,0	5,7

Il GCRI di Georgia è 6,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,3/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Maturità cyber (6,9/10), mentre il più basso è Trasferibilità dati (5,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,3/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Georgia, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Georgia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Georgia, Dal punto di vista italiano, Georgia rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Georgia è indicata una cooperazione selettiva, coerente con il FOTR di 6,3/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasferibilità dati a decisione caso per caso.

Presidi minimi raccomandati

- Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
- Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
- Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
- Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

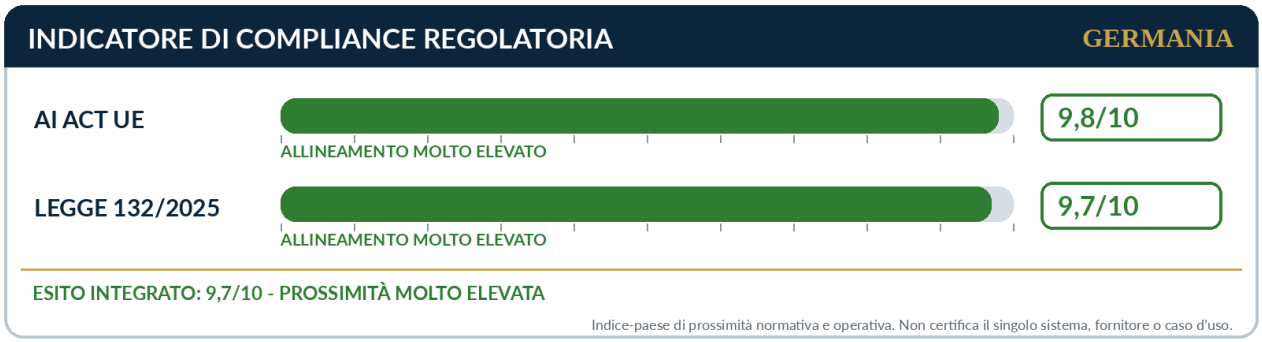
Profilo Celeborn Intelligence di Georgia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati

aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Germania

Posizione FOTR	8	Area	Europa	Subregione	Europa occidentale e centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	9,1	GCRI / 10	8,6	Classe operativa	Affidabilità molto alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Germania, AI Act UE 9,8/10; legge 132/2025 9,7/10; esito integrato 9,7/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Per un operatore italiano, Germania non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 95/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,6/10) e indice FOTR (9,1/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Germania presenta un ecosistema digitale maturo, istituzioni generalmente prevedibili e una buona capacità di gestione degli incidenti. Il rischio residuo deriva soprattutto dalla concentrazione cloud, dalle dipendenze extraeuropee e dalla complessità delle filiere software.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	93,5% / 45,6 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 152.114 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	93,8 / 76,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	97,9/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	78,6/100 - rank 6	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	74/100 - Libero / Libero (95/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,0 / 7,4 / 5,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Germania, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Germania le evidenze principali sono GTMI 76,3/100, EGDI 93,8/100, GCI 97,9/100, AI readiness 78,6/100. La dimensione più robusta è maturità infrastrutturale (9,6/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (7,9/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Germania è 9,6/10. La base statistica rileva utenti Internet pari al 93,5% nel 2024; 45,6 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 152.114 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Germania al posto 6 con un valore medio di 78,6/100; il pilastro migliore è governance (91,2/100), quello più debole è sviluppo e diffusione (66,2/100). Il GTMI 2025 è 76,3/100. Il punteggio S2 è 7,9/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Germania è valutata solida, con S3 pari a 8,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 96,7/100, sviluppo e diffusione dell'IA 66,2/100, penetrazione Internet 93,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Germania ottiene S4 8,0/10 e presenta buona capacità di diversificazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 8,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Germania, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario, luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=8,0/10 e dal proxy di indipendenza 8,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Germania è S5 8,9/10. La base ITU registra ITU GCI 97,9/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure tecniche (17,9/20). Freedom on the Net è 74/100 - Libero, mentre Freedom in the World è Libero (95/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, Bundesdatenschutzgesetz, BSIG e disciplina BSI; quadro NIS2 e regolamenti UE su dati, AI, piattaforme e prodotti con elementi digitali.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,0	Crimini finanziari	7,5
Reti criminali	6,0	Attori incorporati nello Stato	2,0
Attori stranieri	7,5	Attori del settore privato	6,0
Resilienza complessiva	7,4	Cooperazione internazionale	8,0
Politiche e norme nazionali	7,5	Forze dell'ordine	7,5
Antiriciclaggio	6,0	Prevenzione	7,5
Supporto vittime e testimoni	8,0	Rischio operativo FOTR-CY	5,4 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Germania restituisce un rischio FOTR-CY di 5,4/10 (significativo). La componente cyber-dipendente vale 7,0/10 e quella finanziaria 7,5/10; la risposta sistemica è valutata intermedia, con resilienza media di 7,4/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (7,5/10) e reti criminali (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Germania assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Germania, la resilienza complessiva è intermedia (7,4/10); la cooperazione internazionale è robusta (8,0/10), le politiche e norme nazionali sono robuste (7,5/10) e la capacità delle forze dell'ordine è robusta (7,5/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 7,5/10 e supporto a vittime e testimoni 8,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Germania, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Germania. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Germania, In Germania le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. Per i

partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Germania, Il livello governativo di Germania presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Germania, Sul piano militare e dual-use, Germania mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Germania, GDPR, Bundesdatenschutzgesetz, BSIG e disciplina BSI; quadro NIS2 e regolamenti UE su dati, AI, piattaforme e prodotti con elementi digitali. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Germania, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 10,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,6	7,9	8,6	8,0	8,9	8,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,9	8,6	8,1	9,8	8,2	10,0

Il GCRI di Germania è 8,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 9,1/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (10,0/10), mentre il più basso è Trasparenza istituzionale (8,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Basso	Basso	Basso

La matrice applica il FOTR di 9,1/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Germania, la matrice non individua ambiti ad alto rischio; 6 categorie risultano basse o medio-basse, ferma la verifica del singolo progetto. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Germania, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Germania, Dal punto di vista italiano, Germania rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Germania, il FOTR di 9,1/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (8,1/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

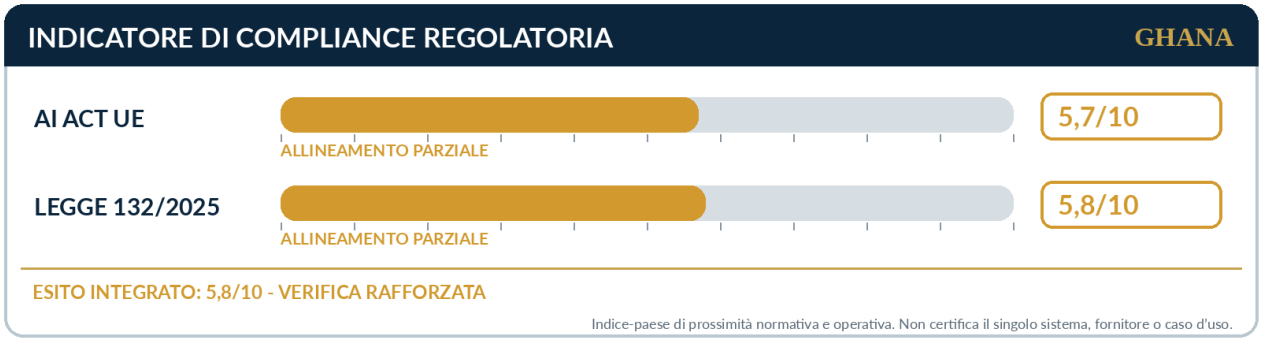
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Germania: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Ghana

Posizione FOTR	82	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,8	GCRI / 10	5,9	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Ghana, AI Act UE 5,7/10; legge 132/2025 5,8/10; esito integrato 5,8/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Ghana è stato membro delle nazioni unite collocato in Africa occidentale. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 80/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,9/10) e indice FOTR (5,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Ghana dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	72,2% / 0,7 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	91,9% / 49 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	63,2 / 70,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	99,3/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	49,1/100 - rank 78	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	64/100 - Parzialmente libero / Libero (80/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 5,3 / 5,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Ghana, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Ghana le evidenze principali sono GTMI 70,8/100, EGDI 63,2/100, GCI 99,3/100, AI readiness 49,1/100. La dimensione più robusta è postura di sicurezza cyber (8,0/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (5,2/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Ghana è 5,7/10. La base statistica rileva utenti Internet pari al 72,2% nel 2024; 0,7 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 91,9% nel 2024; 49 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Ghana al posto 78 con un valore medio di 49,1/100; il pilastro migliore è governance (66,2/100), quello più debole è sviluppo e diffusione (33,7/100). Il GTMI 2025 è 70,8/100. Il punteggio S2 è 5,5/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Ghana è valutata sufficiente ma disomogenea, con S3 pari a 5,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 55,9/100, sviluppo e diffusione dell'IA 33,7/100, penetrazione Internet 72,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Ghana ottiene S4 5,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Ghana, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=5,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Ghana è S5 8,0/10. La base ITU registra ITU GCI 99,3/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è sviluppo delle capacità (19,3/20). Freedom on the Net è 64/100 - Parzialmente libero, mentre Freedom in the World è Libero (80/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Data Protection Act 2012, Cybersecurity Act 2020 e autorità dedicate; livello regionale relativamente strutturato.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	6,5
Reti criminali	7,0	Attori incorporati nello Stato	7,5
Attori stranieri	6,0	Attori del settore privato	5,0
Resilienza complessiva	5,3	Cooperazione internazionale	6,5
Politiche e norme nazionali	5,5	Forze dell'ordine	4,5
Antiriciclaggio	6,0	Prevenzione	4,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	5,7 - SIGNIFICATIVO

Quadro criminale digitale. Per Ghana, l'indice operativo FOTR-CY è 5,7/10, classe significativa. Il mercato dei reati cyber-dipendenti è intermedio (5,0/10), mentre i crimini finanziari sono elevati (6,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,5/10) e reti criminali (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Ghana assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Ghana, la resilienza complessiva è debole (5,3/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Ghana, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Ghana. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Ghana, In Ghana le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Ghana, Il livello governativo di Ghana presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il

settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Ghana, Sul piano militare e dual-use, Ghana mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Ghana, Data Protection Act 2012, Cybersecurity Act 2020 e autorità dedicate; livello regionale relativamente strutturato. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Ghana, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,3/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
5,7	5,5	5,2	5,3	8,0	5,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,0	5,9	5,4	6,5	5,5	5,3

Il GCRI di Ghana è 5,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,5/10), mentre il più basso è Trasferibilità dati (5,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Ghana, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Ghana, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Ghana, Dal punto di vista italiano, Ghana rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Ghana è indicata una cooperazione selettiva, coerente con il FOTR di 5,8/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasferibilità dati a decisione caso per caso.

Presidi minimi raccomandati

- Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
- Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
- Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
- Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

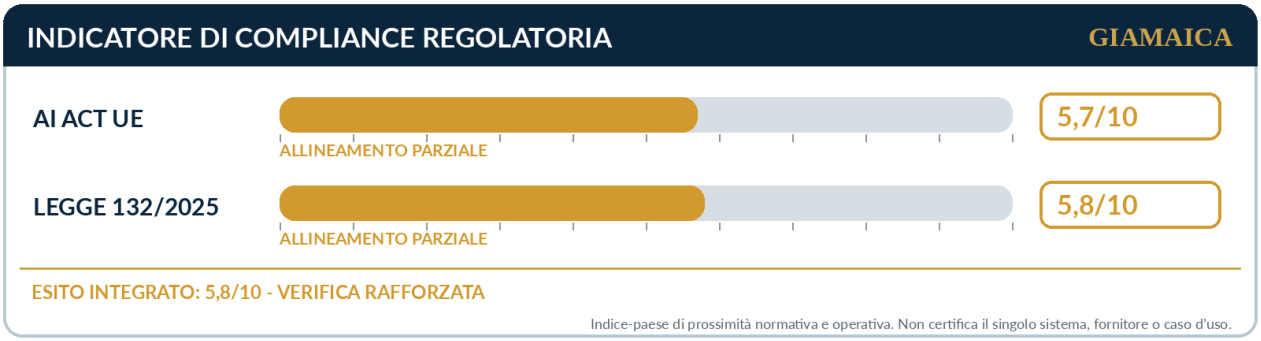
Profilo Celeborn Intelligence di Ghana: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom

House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Giamaica

Posizione FOTR	83	Area	Americhe	Subregione	Caraibi
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,8	GCRI / 10	5,6	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Giamaica, AI Act UE 5,7/10; legge 132/2025 5,8/10; esito integrato 5,8/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Americhe, Giamaica presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 81/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,6/10) e indice FOTR (5,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il quadro di Giamaica è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	90,1% / 16,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	97,7% / 192 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	66,8 / 54,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	58,2/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	43,9/100 - rank 99	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (81/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 5,3 / 6,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Giamaica, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Giamaica le evidenze principali sono GTMI 54,3/100, EGDI 66,8/100, GCI 58,2/100, AI readiness 43,9/100. La dimensione più robusta è maturità infrastrutturale (7,1/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,7/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Giamaica è 7,1/10. La base statistica rileva utenti Internet pari al 90,1% nel 2024; 16,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 97,7% nel 2024; 192 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Giamaica al posto 99 con un valore medio di 43,9/100; il pilastro migliore è governance (64,5/100), quello più debole è sviluppo e diffusione (17,4/100). Il GTMI 2025 è 54,3/100. Il punteggio S2 è 4,7/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Giamaica è valutata sufficiente ma disomogenea, con S3 pari a 5,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 70,6/100, sviluppo e diffusione dell'IA 17,4/100, penetrazione Internet 90,1%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Giamaica ottiene S4 5,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Giamaica, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=5,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Giamaica è S5 5,8/10. La base ITU registra ITU GCI 58,2/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (6,6/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (81/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	7,0
Reti criminali	8,0	Attori incorporati nello Stato	7,5
Attori stranieri	7,0	Attori del settore privato	3,5
Resilienza complessiva	5,3	Cooperazione internazionale	7,0
Politiche e norme nazionali	5,5	Forze dell'ordine	5,5
Antiriciclaggio	5,0	Prevenzione	6,5
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	6,0 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Giamaica presenta un'esposizione stimata significativa (6,0/10): reati cyber-dipendenti 5,0/10, crimini finanziari 7,0/10 e resilienza 5,3/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (8,0/10) e attori incorporati nello Stato (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Giamaica assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Giamaica, la resilienza complessiva è debole (5,3/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 6,5/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Giamaica, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Giamaica. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Giamaica, In Giamaica le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Giamaica, Il livello governativo di Giamaica presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Giamaica, Sul piano militare e dual-use, Giamaica mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Giamaica, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Giamaica, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,4/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,1	4,7	5,5	5,1	5,8	5,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,0	6,0	5,6	6,3	5,6	5,4

Il GCRI di Giamaica è 5,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,3/10), mentre il più basso è Trasferibilità dati (5,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Giamaica, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Giamaica, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Giamaica, Dal punto di vista italiano, Giamaica rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Giamaica è indicata una cooperazione selettiva, coerente con il FOTR di 5,8/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasferibilità dati a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

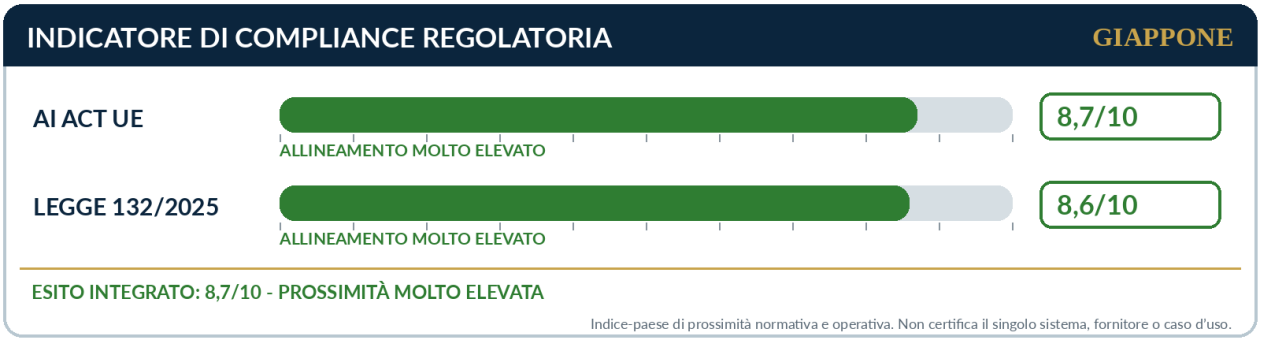
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Giamaica: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Giappone

Posizione FOTR	19	Area	Asia	Subregione	Asia orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	8,8	GCRI / 10	8,6	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Giappone, AI Act UE 8,7/10; legge 132/2025 8,6/10; esito integrato 8,7/10, classe «Allineamento molto elevato». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Giappone, situato in Asia orientale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Asia orientale domestica, Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 96/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,6/10) e indice FOTR (8,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Potenza industriale e digitale con elevata affidabilità, buoni rimedi e decisione UE di adeguatezza; resta necessaria la verifica delle filiere hardware e dei subfornitori asiatici.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	85,5% / 38,6 per 100	2024/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 32.929 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	93,5 / 90,5	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	97,6/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	73,4/100 - rank 14	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	78/100 - Libero / Libero (96/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 7,5 / 4,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Giappone, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Giappone le evidenze principali sono GTMI 90,5/100, EGDI 93,5/100, GCI 97,6/100, AI readiness 73,4/100. La dimensione più robusta è maturità infrastrutturale (9,3/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (7,9/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Giappone è 9,3/10. La base statistica rileva utenti Internet pari al 85,5% nel 2024; 38,6 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 100,0% nel 2024; 32.929 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Giappone al posto 14 con un valore medio di 73,4/100; il pilastro migliore è resilienza (80,8/100), quello più debole è sviluppo e diffusione (66,1/100). Il GTMI 2025 è 90,5/100. Il punteggio S2 è 7,9/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Giappone è valutata solida, con S3 pari a 8,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 91,2/100, sviluppo e diffusione dell'IA 66,1/100, penetrazione Internet 85,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Giappone ottiene S4 8,4/10 e presenta buona capacità di diversificazione. La provenienza prevalente stimata è Asia orientale domestica, Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 8,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Giappone, Fornitura domestica e statunitense, con filiere asiatiche integrate e forte base industriale nazionale. L'impatto sulla valutazione è misurato da S4=8,4/10 e dal proxy di indipendenza 8,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Giappone è S5 9,1/10. La base ITU registra ITU GCI 97,6/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è cooperazione (18,9/20). Freedom on the Net è 78/100 - Libero, mentre Freedom in the World è Libero (96/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Act on the Protection of Personal Information, Basic Act on Cybersecurity e linee guida settoriali; decisione UE di adeguatezza con garanzie supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	6,5
Reti criminali	6,0	Attori incorporati nello Stato	2,0
Attori stranieri	4,5	Attori del settore privato	5,0
Resilienza complessiva	7,5	Cooperazione internazionale	9,0
Politiche e norme nazionali	7,5	Forze dell'ordine	7,5
Antiriciclaggio	7,5	Prevenzione	6,0
Supporto vittime e testimoni	5,5	Rischio operativo FOTR-CY	4,2 - MODERATO

Quadro criminale digitale. Per Giappone, l'indice operativo FOTR-CY è 4,2/10, classe moderata. Il mercato dei reati cyber-dipendenti è intermedio (4,5/10), mentre i crimini finanziari sono elevati (6,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (6,0/10) e attori del settore privato (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Giappone assumono particolare rilevanza compromissioni della supply chain, sottrazione di proprietà intellettuale, furto di cripto-attività, phishing mirato, abuso di identità digitali e intrusioni persistenti contro industria e amministrazioni. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Giappone, la resilienza complessiva è robusta (7,5/10); la cooperazione internazionale è robusta (9,0/10), le politiche e norme nazionali sono robuste (7,5/10) e la capacità delle forze dell'ordine è robusta (7,5/10). Completano il quadro antiriciclaggio 7,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 5,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Giappone, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Giappone. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Giappone, In Giappone le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Giappone, Il livello governativo di Giappone presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Giappone, Sul piano militare e dual-use, Giappone mostra stretta cooperazione con ecosistemi occidentali e capacità dual-use significative. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Giappone, Act on the Protection of Personal Information, Basic Act on Cybersecurity e linee guida settoriali; decisione UE di adeguatezza con garanzie supplementari. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Giappone, È disponibile una decisione UE di adeguatezza. L'operatore italiano deve comunque controllare la portata della decisione, i trasferimenti successivi, le misure di sicurezza e le eventuali discipline settoriali. La componente FOTR di trasferibilità è 10,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,3	7,9	8,1	8,4	9,1	8,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,9	9,7	7,4	7,7	9,1	10,0

Il GCRI di Giappone è 8,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (10,0/10), mentre il più basso è Trasparenza istituzionale (7,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Giappone, la cautela si concentra su 3 ambiti a rischio intermedio: IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Giappone, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Giappone, Dal punto di vista italiano, Giappone rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Giappone, il FOTR di 8,8/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (7,4/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

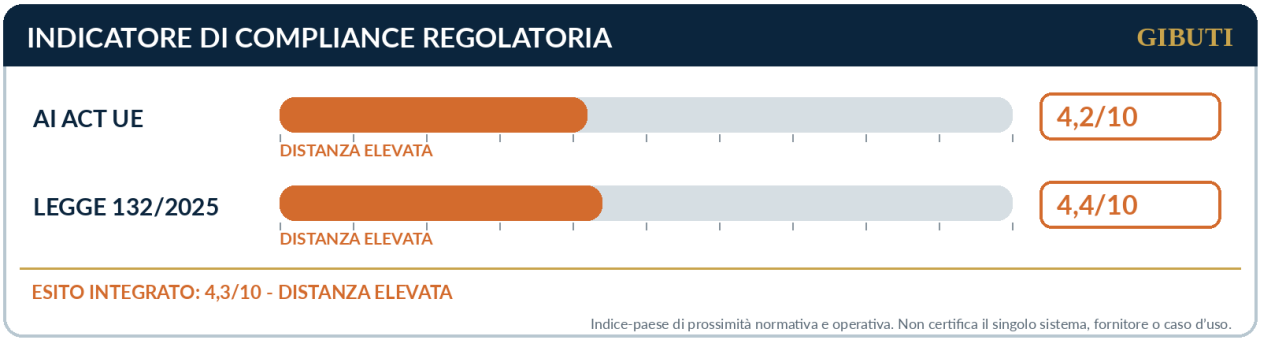
Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Giappone: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Gibuti

Posizione FOTR	147	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,5	GCRI / 10	3,4	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Gibuti, AI Act UE 4,2/10; legge 132/2025 4,4/10; esito integrato 4,3/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Per un operatore italiano, Gibuti non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 24/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (4,5/10) supera il GCRI tecnico (3,4/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Gibuti è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	65,3% / 1,5 per 100	2024/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	69,2% / 115 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	29,1 / 16,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	31,5/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	22,5/100 - rank 148	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (24/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 4,1 / 5,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Gibuti, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Gibuti le evidenze principali sono GTMI 16,9/100, EGDI 29,1/100, GCI 31,5/100, AI readiness 22,5/100. La dimensione più robusta è maturità infrastrutturale (4,3/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,3/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Gibuti è 4,3/10. La base statistica rileva utenti Internet pari al 65,3% nel 2024; 1,5 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 69,2% nel 2024; 115 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Gibuti al posto 148 con un valore medio di 22,5/100; il pilastro migliore è infrastrutture IA (37,7/100), quello più debole è politiche pubbliche (11,5/100). Il GTMI 2025 è 16,9/100. Il punteggio S2 è 2,3/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Gibuti è valutata fragile, con S3 pari a 2,7/10. Le evidenze disponibili comprendono indice UN di capitale umano 28,0/100, sviluppo e diffusione dell'IA 22,8/100, penetrazione Internet 65,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Gibuti ottiene S4 4,3/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Gibuti, Presenza cinese, europea, statunitense e regionale, condizionata dalla posizione strategica del Paese. L'impatto sulla valutazione è misurato da S4=4,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Gibuti è S5 3,6/10. La base ITU registra ITU GCI 31,5/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è sviluppo delle capacità (1,7/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (24/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	6,5
Reti criminali	6,0	Attori incorporati nello Stato	6,0
Attori stranieri	7,0	Attori del settore privato	6,0
Resilienza complessiva	4,1	Cooperazione internazionale	6,5
Politiche e norme nazionali	4,5	Forze dell'ordine	4,0
Antiriciclaggio	5,0	Prevenzione	4,0
Supporto vittime e testimoni	2,5	Rischio operativo FOTR-CY	5,0 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (2,0/10), criminalità finanziaria (6,5/10) e resilienza (4,1/10) colloca Gibuti in una fascia di rischio significativo, pari a 5,0/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (7,0/10) e reti criminali (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Gibuti assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Gibuti, la resilienza complessiva è debole (4,1/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono deboli (4,5/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 2,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Gibuti, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Gibuti. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Gibuti, In Gibuti le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità

del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Gibuti, Il livello governativo di Gibuti presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Gibuti, Sul piano militare e dual-use, Gibuti mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Gibuti, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Gibuti, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,3/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
4,3	2,3	2,7	4,3	3,6	3,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,4	4,5	4,4	5,2	4,0	4,3

Il GCRI di Gibuti è 3,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,2/10), mentre il più basso è Supply chain (4,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Gibuti, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Gibuti, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Gibuti, Dal punto di vista italiano, Gibuti rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Gibuti ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

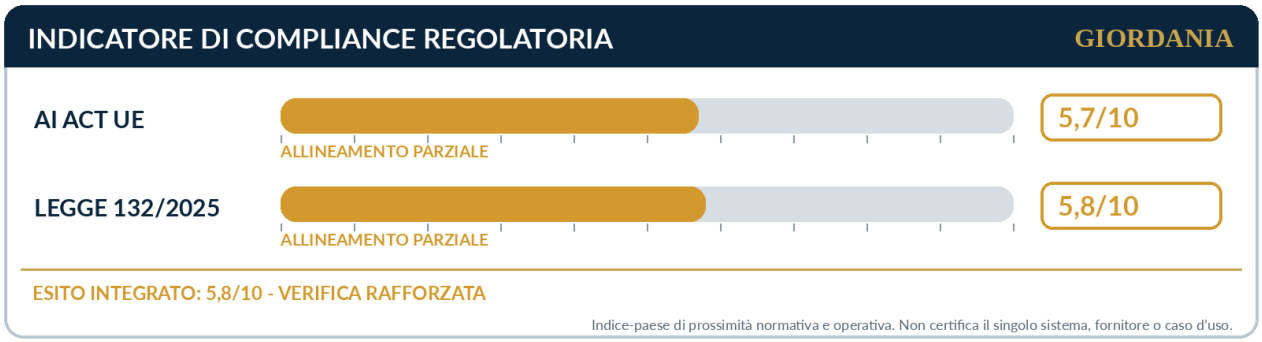
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Gibuti: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Giordania

Posizione FOTR	97	Area	Asia	Subregione	Medio Oriente e Asia occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,7	GCRI / 10	6,4	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Giordania, AI Act UE 5,7/10; legge 132/2025 5,8/10; esito integrato 5,8/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Giordania è stato membro delle nazioni unite collocato in Medio Oriente e Asia occidentale. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 34/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,4/10) e indice FOTR (5,7/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Giordania dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	95,6% / 7,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 212 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	68,5 / 91,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	98,6/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	60,0/100 - rank 63	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	47/100 - Parzialmente libero / Parzialmente libero (34/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 5,6 / 5,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Giordania, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Giordania le evidenze principali sono GTMI 91,4/100, EGDI 68,5/100, GCI 98,6/100, AI readiness 60,0/100. La dimensione più robusta è postura di sicurezza cyber (7,6/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (5,6/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Giordania è 6,6/10. La base statistica rileva utenti Internet pari al 95,6% nel 2024; 7,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 212 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Giordania al posto 63 con un valore medio di 60,0/100; il pilastro migliore è adozione pubblica (80,0/100), quello più debole è sviluppo e diffusione (35,5/100). Il GTMI 2025 è 91,4/100. Il punteggio S2 è 6,7/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Giordania è valutata sufficiente ma disomogenea, con S3 pari a 5,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 64,6/100, sviluppo e diffusione dell'IA 35,5/100, penetrazione Internet 95,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Giordania ottiene S4 5,6/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Giordania, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo societario e subfornitura. L'impatto sulla valutazione è misurato da S4=5,6/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Giordania è S5 7,6/10. La base ITU registra ITU GCI 98,6/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è organizzazione (19,2/20). Freedom on the Net è 47/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (34/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Personal Data Protection Law 24/2023 e quadro cyber nazionale; sistema recente, da valutare rispetto a regolamenti e prassi applicative.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	6,5
Reti criminali	7,0	Attori incorporati nello Stato	6,0
Attori stranieri	5,5	Attori del settore privato	6,0
Resilienza complessiva	5,6	Cooperazione internazionale	8,0
Politiche e norme nazionali	6,5	Forze dell'ordine	6,5
Antiriciclaggio	7,0	Prevenzione	6,5
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	5,6 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Giordania il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,6/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 5,5/10; le frodi e i reati finanziari 6,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (7,0/10) e attori incorporati nello Stato (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Giordania assumono particolare rilevanza phishing e credential theft, ransomware, frodi d'investimento, attacchi a energia e servizi pubblici, abuso di cripto-attività e campagne che possono combinare profitto, spionaggio e pressione politica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Giordania, la resilienza complessiva è intermedia (5,6/10); la cooperazione internazionale è robusta (8,0/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è intermedia (6,5/10). Completano il quadro antiriciclaggio 7,0/10, prevenzione 6,5/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Giordania, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Giordania. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Giordania, In Giordania le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Giordania, Il livello governativo di Giordania presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Giordania, Sul piano militare e dual-use, Giordania mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Giordania, Personal Data Protection Law 24/2023 e quadro cyber nazionale; sistema recente, da valutare rispetto a regolamenti e prassi applicative. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Giordania, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,2/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,6	6,7	5,6	5,6	7,6	6,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,7	6,4	5,1	5,8	5,9	5,2

Il GCRI di Giordania è 6,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (6,4/10), mentre il più basso è Trasparenza istituzionale (5,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Giordania, 1 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Giordania, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Giordania, Dal punto di vista italiano, Giordania rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Giordania è indicata una cooperazione selettiva, coerente con il FOTR di 5,7/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

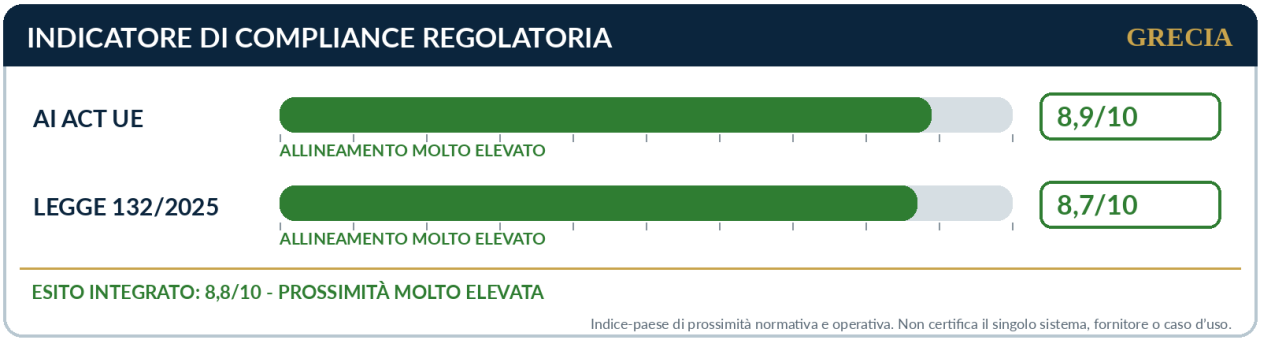
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Giordania: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Grecia

Posizione FOTR	36	Area	Europa	Subregione	Europa sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,1	GCRI / 10	7,7	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Grecia, AI Act UE 8,9/10; legge 132/2025 8,7/10; esito integrato 8,8/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Nel quadro di Europa, Grecia presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 85/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,7/10) e indice FOTR (8,1/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ambiente digitale di Grecia è complessivamente affidabile e aperto agli scambi. Per investimenti italiani è opportuno verificare la disciplina locale, la struttura dei fornitori e gli eventuali poteri pubblici di accesso.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	86,3% / 44,7 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 15.658 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	86,7 / 88,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	97,1/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	64,5/100 - rank 42	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (85/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 5,1 / 5,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Grecia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Grecia le evidenze principali sono GTMI 88,3/100, EGDI 86,7/100, GCI 97,1/100, AI readiness 64,5/100. La dimensione più robusta è maturità infrastrutturale (9,0/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,0/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Grecia è 9,0/10. La base statistica rileva utenti Internet pari al 86,3% nel 2024; 44,7 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 15.658 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Grecia al posto 42 con un valore medio di 64,5/100; il pilastro migliore è adozione pubblica (78,8/100), quello più debole è sviluppo e diffusione (41,5/100). Il GTMI 2025 è 88,3/100. Il punteggio S2 è 7,0/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Grecia è valutata sufficiente ma disomogenea, con S3 pari a 7,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 92,2/100, sviluppo e diffusione dell'IA 41,5/100, penetrazione Internet 86,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Grecia ottiene S4 6,0/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Grecia, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,0/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Grecia è S5 9,0/10. La base ITU registra ITU GCI 97,1/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è sviluppo delle capacità (17,9/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (85/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, legge 4624/2019 e disciplina nazionale di cybersicurezza; quadro UE pienamente applicabile.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	6,5
Reti criminali	6,5	Attori incorporati nello Stato	7,5
Attori stranieri	6,5	Attori del settore privato	6,5
Resilienza complessiva	5,1	Cooperazione internazionale	7,0
Politiche e norme nazionali	6,0	Forze dell'ordine	5,0
Antiriciclaggio	5,5	Prevenzione	5,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	5,6 - SIGNIFICATIVO

Quadro criminale digitale. Per Grecia, l'indice operativo FOTR-CY è 5,6/10, classe significativa. Il mercato dei reati cyber-dipendenti è intermedio (4,5/10), mentre i crimini finanziari sono elevati (6,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,5/10) e reti criminali (6,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Grecia assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Grecia, la resilienza complessiva è debole (5,1/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 5,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Grecia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Grecia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Grecia, In Grecia le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Grecia, Il livello governativo di Grecia presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Grecia, Sul piano militare e dual-use, Grecia mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Grecia, GDPR, legge 4624/2019 e disciplina nazionale di cybersicurezza; quadro UE pienamente applicabile. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Grecia, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 8,8/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,0	7,0	7,5	6,0	9,0	7,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,5	7,8	7,6	8,6	7,0	8,8

Il GCRI di Grecia è 7,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,1/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (8,8/10), mentre il più basso è Supply chain (7,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,1/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Grecia, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Grecia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Grecia, Dal punto di vista italiano, Grecia rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Grecia, il FOTR di 8,1/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (7,0/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

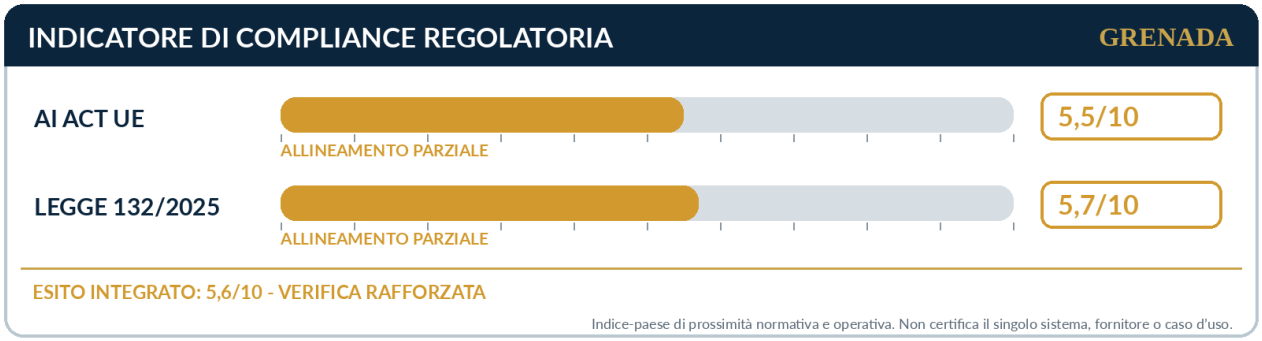
Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Grecia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Grenada

Posizione FOTR	84	Area	Americhe	Subregione	Caraibi
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,8	GCRI / 10	4,5	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Grenada, AI Act UE 5,5/10; legge 132/2025 5,7/10; esito integrato 5,6/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Grenada, situato in Caraibi, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 89/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,8/10) supera il GCRI tecnico (4,5/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. In Grenada la trasformazione digitale procede più rapidamente dell'uniformità regolatoria e operativa. Gli investimenti devono essere accompagnati da audit, clausole di uscita e gestione locale del rischio.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	70,2% / 29,8 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	95,6% / 742 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	64,6 / 30,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	20,1/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	17,8/100 - rank 176	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (89/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 5,2 / 3,3	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Grenada, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Grenada le evidenze principali sono GTMI 30,6/100, EGDI 64,6/100, GCI 20,1/100, AI readiness 17,8/100. La dimensione più robusta è maturità infrastrutturale (7,2/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,6/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Grenada è 7,2/10. La base statistica rileva utenti Internet pari al 70,2% nel 2024; 29,8 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 95,6% nel 2024; 742 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Grenada al posto 176 con un valore medio di 17,8/100; il pilastro migliore è infrastrutture IA (32,4/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 30,6/100. Il punteggio S2 è 2,6/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Grenada è valutata sufficiente ma disomogenea, con S3 pari a 5,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 75,5/100, sviluppo e diffusione dell'IA 12,0/100, penetrazione Internet 70,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Grenada ottiene S4 4,4/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Grenada, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=4,4/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Grenada è S5 3,3/10. La base ITU registra ITU GCI 20,1/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (89/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	3,0
Reti criminali	3,0	Attori incorporati nello Stato	3,5
Attori stranieri	4,0	Attori del settore privato	3,5
Resilienza complessiva	5,2	Cooperazione internazionale	6,0
Politiche e norme nazionali	5,5	Forze dell'ordine	6,5
Antiriciclaggio	5,0	Prevenzione	4,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	3,3 - MODERATO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (2,0/10), criminalità finanziaria (3,0/10) e resilienza (5,2/10) colloca Grenada in una fascia di rischio moderato, pari a 3,3/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (4,0/10) e attori incorporati nello Stato (3,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Grenada assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Grenada, la resilienza complessiva è debole (5,2/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è intermedia (6,5/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Grenada, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Grenada. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Grenada, In Grenada le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Grenada, Il livello governativo di Grenada presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il

settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Grenada, Sul piano militare e dual-use, Grenada mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Grenada, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Grenada, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,8/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,2	2,6	5,0	4,4	3,3	4,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,7	5,5	6,1	6,3	5,5	5,8

Il GCRI di Grenada è 4,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,3/10), mentre il più basso è Maturità cyber (5,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Grenada, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Grenada, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Grenada, Dal punto di vista italiano, Grenada rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Grenada è indicata una cooperazione selettiva, coerente con il FOTR di 5,8/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Maturità cyber a decisione caso per caso.

Presidi minimi raccomandati

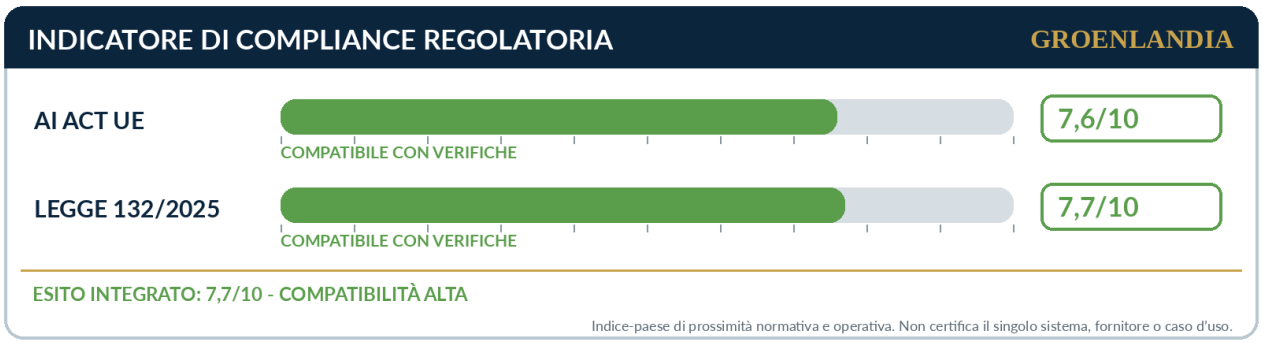
Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Grenada: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Groenlandia

Posizione FOTR	45	Area	Artico	Subregione	Artico nordamericano
Status	Territorio autonomo del Regno di Danimarca	Confidenza Celeborn Intelligence	Media	Copertura dati	3/7 famiglie
FOTR / 10	7,6	GCRI / 10	7,3	Classe operativa	Affidabilità favorevole ma condizionata

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Groenlandia, AI Act UE 7,6/10; legge 132/2025 7,7/10; esito integrato 7,7/10, classe «Compatibile con verifiche». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Prima dell'ingaggio occorre una analisi degli scostamenti mirata su trasparenza, governance dei dati, rappresentanza nell'UE, audit e rimedi contrattuali.

Premessa geopolitica e tecnologica

Per un operatore italiano, Groenlandia non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La posizione internazionale e il modello di governance digitale devono essere considerati insieme alla maturità tecnica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Per questa entità non è disponibile un indicatore Freedom in the World direttamente comparabile; l'assenza di copertura viene trattata come limite informativo e non come prova automatica di rischio. GCRI tecnico (7,3/10) e indice FOTR (7,6/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Territorio artico strategico, con limitata scala locale e forte dipendenza dal Regno di Danimarca, dalle telecomunicazioni satellitari e dai collegamenti sottomarini.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	69,5% / 32,0 per 100	2017/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 3.906 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	n.d. / n.d.	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	n.d./100 - n.d.	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	n.d./100 - rank n.d.	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / n.d.	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,6 / 8,0 / 4,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Groenlandia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 3/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Groenlandia le evidenze principali sono nessun indicatore composito pienamente comparabile. La dimensione più robusta è maturità infrastrutturale (7,8/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,7/10). Sono disponibili 3 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata media. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Groenlandia è 7,8/10. La base statistica rileva utenti Internet pari al 69,5% nel 2017; 32,0 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 100,0% nel 2024; 3.906 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Per Groenlandia non è disponibile un profilo Oxford Insights direttamente attribuibile; l'adozione di IA è quindi valutata attraverso GovTech, servizi online, infrastrutture e fonti qualitative. Il punteggio S2 è 7,5/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Groenlandia è valutata sufficiente ma disomogenea, con S3 pari a 7,8/10. Le evidenze disponibili comprendono penetrazione Internet 69,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Groenlandia ottiene S4 5,7/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Groenlandia, Dipendenza prevalente da Danimarca, operatori nordici, Stati Uniti e infrastrutture satellitari/sottomarine. L'impatto sulla valutazione è misurato da S4=5,7/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Groenlandia è S5 7,5/10. La base ITU registra GCI non disponibile in forma comparabile. Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è n.d.. Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo non pienamente comparabile al GDPR; necessaria una verifica locale aggiornata su privacy, cybersicurezza, accessi pubblici e trasferimenti internazionali.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,6	Crimini finanziari	5,4
Reti criminali	5,0	Attori incorporati nello Stato	1,6
Attori stranieri	5,3	Attori del settore privato	2,9
Resilienza complessiva	8,0	Cooperazione internazionale	8,1
Politiche e norme nazionali	8,8	Forze dell'ordine	7,9
Antiriciclaggio	6,8	Prevenzione	8,1
Supporto vittime e testimoni	7,7	Rischio operativo FOTR-CY	4,6 - MODERATO

Quadro criminale digitale. Per Groenlandia, l'indice operativo FOTR-CY è 4,6/10, classe moderata. Il mercato dei reati cyber-dipendenti è elevato (6,6/10), mentre i crimini finanziari sono intermedi (5,4/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (5,3/10) e reti criminali (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Groenlandia assumono particolare rilevanza ransomware, phishing, furto di credenziali, frodi finanziarie, compromissione di terze parti, estorsione dei dati e riciclaggio digitale transfrontaliero. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Groenlandia, la resilienza complessiva è robusta (8,0/10); la cooperazione internazionale è robusta (8,1/10), le politiche e norme nazionali sono robuste (8,8/10) e la capacità delle forze dell'ordine è robusta (7,9/10). Completano il quadro antiriciclaggio 6,8/10, prevenzione 8,1/10 e supporto a vittime e testimoni 7,7/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Groenlandia, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova. Poiché l'entità non dispone di una serie nazionale GI-TOC autonoma, i valori derivano da un proxy Celeborn Intelligence ponderato su Danimarca 80%, Canada 20%; la confidenza deve pertanto essere considerata inferiore e la decisione resa più prudente.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; proxy Celeborn Intelligence ponderato su Danimarca 80%, Canada 20%. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Groenlandia, In Groenlandia le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Groenlandia, Il livello governativo di Groenlandia presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Groenlandia, Sul piano militare e dual-use, Groenlandia mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Groenlandia, Quadro normativo non pienamente comparabile al GDPR; necessaria una verifica locale aggiornata su privacy, cybersicurezza, accessi pubblici e trasferimenti internazionali. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Groenlandia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 7,3/10 e il rischio sui dati personali è Medio-basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,8	7,5	7,8	5,7	7,5	7,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
7,9	7,3	7,8	8,3	7,0	7,3

Il GCRI di Groenlandia è 7,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 7,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (8,3/10), mentre il più basso è Supply chain (7,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 7,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Groenlandia, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Groenlandia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Groenlandia, Dal punto di vista italiano, Groenlandia rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Groenlandia è favorevole ma condizionata: il valore FOTR di 7,6/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Supply chain.

Presidi minimi raccomandati

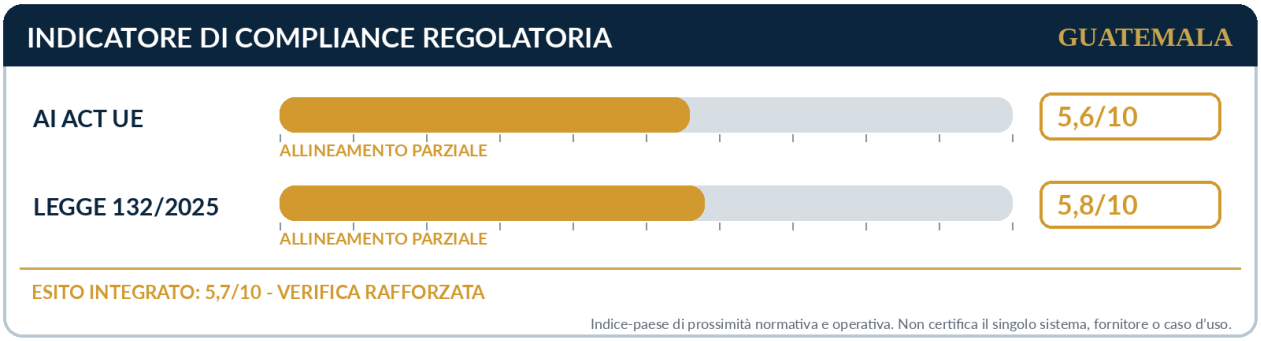
- Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
- Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
- Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
- Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Groenlandia: World Development Indicators, valori più recenti disponibili 2022-2024; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Media con copertura 3/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Guatemala

Posizione FOTR	85	Area	Americhe	Subregione	America centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,8	GCRI / 10	4,6	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Guatemala, AI Act UE 5,6/10; legge 132/2025 5,8/10; esito integrato 5,7/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Guatemala è stato membro delle nazioni unite collocato in America centrale. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 48/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,8/10) supera il GCRI tecnico (4,6/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il quadro di Guatemala è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	60,2% / 5,3 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	90,9% / 109 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	57,4 / 57,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	40,0/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	29,6/100 - rank 129	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (48/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Firmatario/invitato	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 4,0 / 6,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Guatemala, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Guatemala le evidenze principali sono GTMI 57,3/100, EGDI 57,4/100, GCI 40,0/100, AI readiness 29,6/100. La dimensione più robusta è maturità infrastrutturale (5,3/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,0/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Guatemala è 5,3/10. La base statistica rileva utenti Internet pari al 60,2% nel 2024; 5,3 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 90,9% nel 2024; 109 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Guatemala al posto 129 con un valore medio di 29,6/100; il pilastro migliore è governance (44,5/100), quello più debole è sviluppo e diffusione (11,9/100). Il GTMI 2025 è 57,3/100. Il punteggio S2 è 4,0/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Guatemala è valutata fragile, con S3 pari a 4,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 48,3/100, sviluppo e diffusione dell'IA 11,9/100, penetrazione Internet 60,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Guatemala ottiene S4 5,0/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Guatemala, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=5,0/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Guatemala è S5 4,6/10. La base ITU registra ITU GCI 40,0/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (3,8/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (48/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Firmatario/invitato. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	7,0
Reti criminali	6,0	Attori incorporati nello Stato	8,0
Attori stranieri	8,0	Attori del settore privato	6,5
Resilienza complessiva	4,0	Cooperazione internazionale	5,5
Politiche e norme nazionali	4,5	Forze dell'ordine	5,5
Antiriciclaggio	4,0	Prevenzione	4,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	6,2 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Guatemala restituisce un rischio FOTR-CY di 6,2/10 (significativo). La componente cyber-dipendente vale 5,0/10 e quella finanziaria 7,0/10; la risposta sistemica è valutata debole, con resilienza media di 4,0/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e attori stranieri (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Guatemala assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Guatemala, la resilienza complessiva è debole (4,0/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono deboli (4,5/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Guatemala, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Guatemala. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Guatemala, In Guatemala le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Guatemala, Il livello governativo di Guatemala presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Guatemala, Sul piano militare e dual-use, Guatemala mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Guatemala, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Firmatario/invitato; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Guatemala, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,5/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
5,3	4,0	4,1	5,0	4,6	4,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,8	5,7	5,9	6,1	6,0	5,5

Il GCRI di Guatemala è 4,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,1/10), mentre il più basso è Trasferibilità dati (5,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Guatemala, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Guatemala, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Guatemala, Dal punto di vista italiano, Guatemala rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Guatemala è indicata una cooperazione selettiva, coerente con il FOTR di 5,8/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasferibilità dati a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

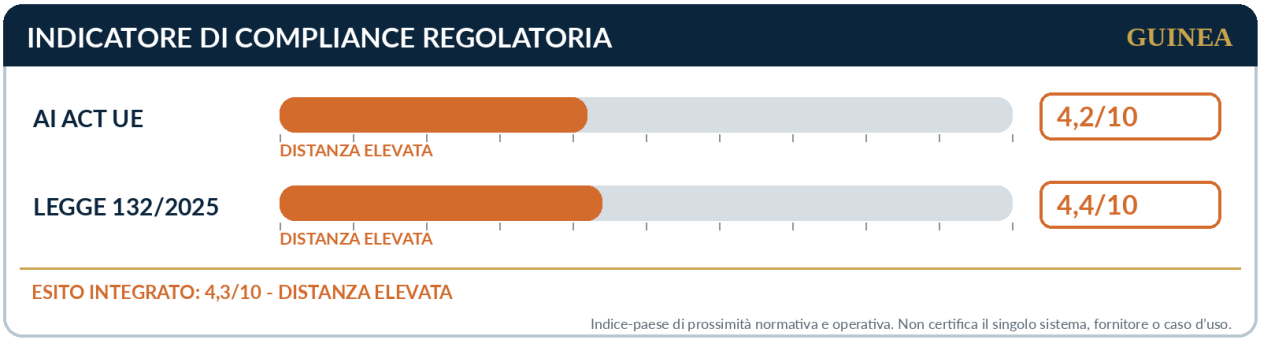
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Guatemala: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Guinea

Posizione FOTR	164	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,4	GCRI / 10	3,7	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Guinea, AI Act UE 4,2/10; legge 132/2025 4,4/10; esito integrato 4,3/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Guinea presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 28/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (3,7/10) e indice FOTR (4,4/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Guinea è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	33,3% / 0,0 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	53,8% / 12 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	40,1 / 51,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	56,4/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	17,3/100 - rank 183	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (28/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 3,0 / 5,3	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Guinea, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Guinea le evidenze principali sono GTMI 51,0/100, EGDI 40,1/100, GCI 56,4/100, AI readiness 17,3/100. La dimensione più robusta è postura di sicurezza cyber (5,1/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (2,5/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Guinea è 3,2/10. La base statistica rileva utenti Internet pari al 33,3% nel 2024; 0,0 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 53,8% nel 2024; 12 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Guinea al posto 183 con un valore medio di 17,3/100; il pilastro migliore è resilienza (32,8/100), quello più debole è politiche pubbliche (4,0/100). Il GTMI 2025 è 51,0/100. Il punteggio S2 è 2,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Guinea è valutata fragile, con S3 pari a 2,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 28,9/100, sviluppo e diffusione dell'IA 11,6/100, penetrazione Internet 33,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Guinea ottiene S4 4,7/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Guinea, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,7/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Guinea è S5 5,1/10. La base ITU registra ITU GCI 56,4/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (4,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (28/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	5,5
Reti criminali	6,5	Attori incorporati nello Stato	8,0
Attori stranieri	6,5	Attori del settore privato	4,0
Resilienza complessiva	3,0	Cooperazione internazionale	3,5
Politiche e norme nazionali	3,0	Forze dell'ordine	3,0
Antiriciclaggio	3,0	Prevenzione	3,0
Supporto vittime e testimoni	2,5	Rischio operativo FOTR-CY	5,3 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Guinea presenta un'esposizione stimata significativa (5,3/10): reati cyber-dipendenti 2,0/10, crimini finanziari 5,5/10 e resilienza 3,0/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e reti criminali (6,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Guinea assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Guinea, la resilienza complessiva è molto debole (3,0/10); la cooperazione internazionale è debole (3,5/10), le politiche e norme nazionali sono molto deboli (3,0/10) e la capacità delle forze dell'ordine è molto debole (3,0/10). Completano il quadro antiriciclaggio 3,0/10, prevenzione 3,0/10 e supporto a vittime e testimoni 2,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Guinea, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Guinea. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Guinea, In Guinea le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La superficie di

rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Guinea, Il livello governativo di Guinea presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Guinea, Sul piano militare e dual-use, Guinea mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Guinea, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Guinea, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,1/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,2	2,9	2,5	4,7	5,1	3,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,4	4,2	4,2	5,1	4,3	4,1

Il GCRI di Guinea è 3,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,1/10), mentre il più basso è Trasferibilità dati (4,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Guinea, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Guinea, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Guinea, Dal punto di vista italiano, Guinea rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Guinea ricade nella fascia di alto rischio (4,4/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

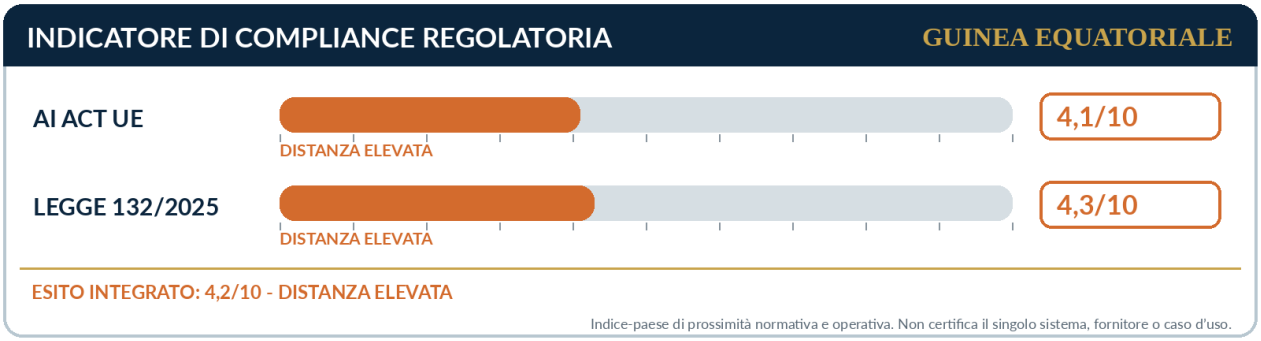
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Guinea: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Guinea Equatoriale

Posizione FOTR	165	Area	Africa	Subregione	Africa centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,4	GCRI / 10	3,1	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Guinea Equatoriale, AI Act UE 4,1/10; legge 132/2025 4,3/10; esito integrato 4,2/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Guinea Equatoriale, situato in Africa centrale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 5/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (4,4/10) supera il GCRI tecnico (3,1/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Guinea Equatoriale è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	63,3% / 0,1 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	65,1% / 67 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	28,6 / 12,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	25,4/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	15,0/100 - rank 187	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (5/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	1,0 / 2,1 / 5,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Guinea Equatoriale, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Guinea Equatoriale le evidenze principali sono GTMI 12,6/100, EGDI 28,6/100, GCI 25,4/100, AI readiness 15,0/100. La dimensione più robusta è indipendenza della supply chain (4,2/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (1,6/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Guinea Equatoriale è 3,6/10. La base statistica rileva utenti Internet pari al 63,3% nel 2024; 0,1 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 65,1% nel 2024; 67 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Guinea Equatoriale al posto 187 con un valore medio di 15,0/100; il pilastro migliore è infrastrutture IA (28,1/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 12,6/100. Il punteggio S2 è 1,6/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Guinea Equatoriale è valutata fragile, con S3 pari a 3,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 41,0/100, sviluppo e diffusione dell'IA 12,7/100, penetrazione Internet 63,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Guinea Equatoriale ottiene S4 4,2/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Guinea Equatoriale, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre

ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,2/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Guinea Equatoriale è S5 3,2/10. La base ITU registra ITU GCI 25,4/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (1,4/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (5/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	1,0	Crimini finanziari	7,0
Reti criminali	2,0	Attori incorporati nello Stato	9,0
Attori stranieri	5,5	Attori del settore privato	8,5
Resilienza complessiva	2,1	Cooperazione internazionale	2,5
Politiche e norme nazionali	3,5	Forze dell'ordine	2,0
Antiriciclaggio	2,0	Prevenzione	2,0
Supporto vittime e testimoni	1,5	Rischio operativo FOTR-CY	5,0 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (1,0/10), criminalità finanziaria (7,0/10) e resilienza (2,1/10) colloca Guinea Equatoriale in una fascia di rischio significativo, pari a 5,0/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e attori del settore privato (8,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Guinea Equatoriale assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Guinea Equatoriale, la resilienza complessiva è molto debole (2,1/10); la cooperazione internazionale è molto debole (2,5/10), le politiche e norme nazionali sono deboli (3,5/10) e la capacità delle forze dell'ordine è molto debole (2,0/10). Completano il quadro antiriciclaggio 2,0/10, prevenzione 2,0/10 e supporto a vittime e testimoni 1,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Guinea Equatoriale, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Guinea Equatoriale. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Guinea Equatoriale, In Guinea Equatoriale le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi

operatori. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Guinea Equatoriale, Il livello governativo di Guinea Equatoriale presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Guinea Equatoriale, Sul piano militare e dual-use, Guinea Equatoriale mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Guinea Equatoriale, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Guinea Equatoriale, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,1/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,6	1,6	3,1	4,2	3,2	3,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,4	4,3	4,3	5,1	4,2	4,1

Il GCRI di Guinea Equatoriale è 3,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,1/10), mentre il più basso è Trasferibilità dati (4,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Guinea Equatoriale, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Guinea Equatoriale, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Guinea Equatoriale, Dal punto di vista italiano, Guinea Equatoriale rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Guinea Equatoriale ricade nella fascia di alto rischio (4,4/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

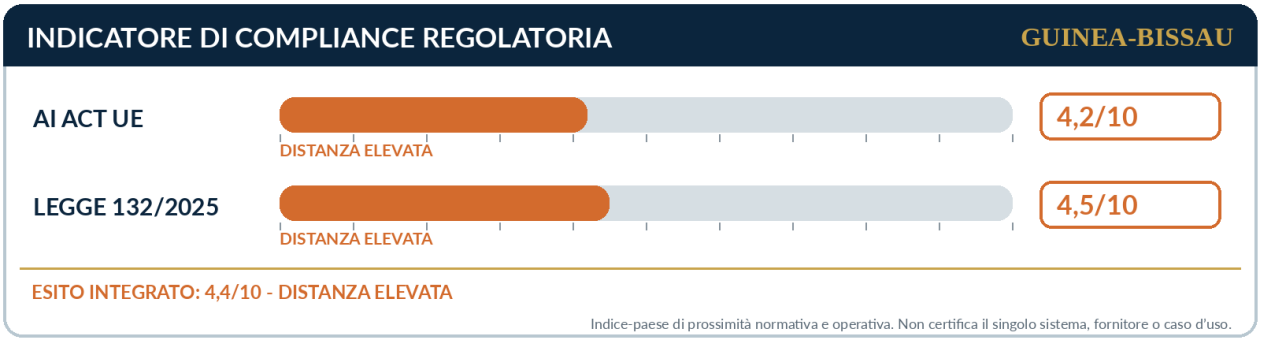
Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.
Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Guinea Equatoriale: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Guinea-Bissau

Posizione FOTR	139	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,6	GCRI / 10	2,7	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Guinea-Bissau, AI Act UE 4,2/10; legge 132/2025 4,5/10; esito integrato 4,4/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Per un operatore italiano, Guinea-Bissau non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 33/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (4,6/10) supera il GCRI tecnico (2,7/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Guinea-Bissau presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	29,8% / 0,4 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	43,7% / 11 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	30,8 / 17,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	6,4/100 - Tier 5 - capacità iniziali	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	10,8/100 - rank 195	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (33/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 2,7 / 5,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Guinea-Bissau, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Guinea-Bissau le evidenze principali sono GTMI 17,7/100, EGDI 30,8/100, GCI 6,4/100, AI readiness 10,8/100. La dimensione più robusta è indipendenza della supply chain (4,4/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (1,4/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Guinea-Bissau è 3,2/10. La base statistica rileva utenti Internet pari al 29,8% nel 2024; 0,4 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 43,7% nel 2024; 11 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Guinea-Bissau al posto 195 con un valore medio di 10,8/100; il pilastro migliore è infrastrutture IA (23,2/100), quello più debole è adozione pubblica (2,0/100). Il GTMI 2025 è 17,7/100. Il punteggio S2 è 1,4/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Guinea-Bissau è valutata fragile, con S3 pari a 2,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 30,8/100, sviluppo e diffusione dell'IA 10,5/100, penetrazione Internet 29,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Guinea-Bissau ottiene S4 4,4/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Guinea-Bissau, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre

ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,4/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Guinea-Bissau è S5 2,1/10. La base ITU registra ITU GCI 6,4/100, Tier 5 - capacità iniziali; il pilastro relativamente più debole è misure giuridiche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (33/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	6,0
Reti criminali	8,0	Attori incorporati nello Stato	8,5
Attori stranieri	6,5	Attori del settore privato	4,0
Resilienza complessiva	2,7	Cooperazione internazionale	4,0
Politiche e norme nazionali	3,0	Forze dell'ordine	3,0
Antiriciclaggio	3,0	Prevenzione	2,0
Supporto vittime e testimoni	1,5	Rischio operativo FOTR-CY	5,6 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (2,0/10), criminalità finanziaria (6,0/10) e resilienza (2,7/10) colloca Guinea-Bissau in una fascia di rischio significativo, pari a 5,6/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,5/10) e reti criminali (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Guinea-Bissau assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Guinea-Bissau, la resilienza complessiva è molto debole (2,7/10); la cooperazione internazionale è debole (4,0/10), le politiche e norme nazionali sono molto deboli (3,0/10) e la capacità delle forze dell'ordine è molto debole (3,0/10). Completano il quadro antiriciclaggio 3,0/10, prevenzione 2,0/10 e supporto a vittime e testimoni 1,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Guinea-Bissau, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Guinea-Bissau. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Guinea-Bissau, In Guinea-Bissau le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i

partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Guinea-Bissau, Il livello governativo di Guinea-Bissau presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Guinea-Bissau, Sul piano militare e dual-use, Guinea-Bissau mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Guinea-Bissau, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Guinea-Bissau, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,4/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,2	1,4	2,5	4,4	2,1	2,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,5	4,6	4,5	5,3	4,4	4,4

Il GCRI di Guinea-Bissau è 2,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,3/10), mentre il più basso è Supply chain (4,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Guinea-Bissau, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Guinea-Bissau, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Guinea-Bissau, Dal punto di vista italiano, Guinea-Bissau rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Guinea-Bissau ricade nella fascia di alto rischio (4,6/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

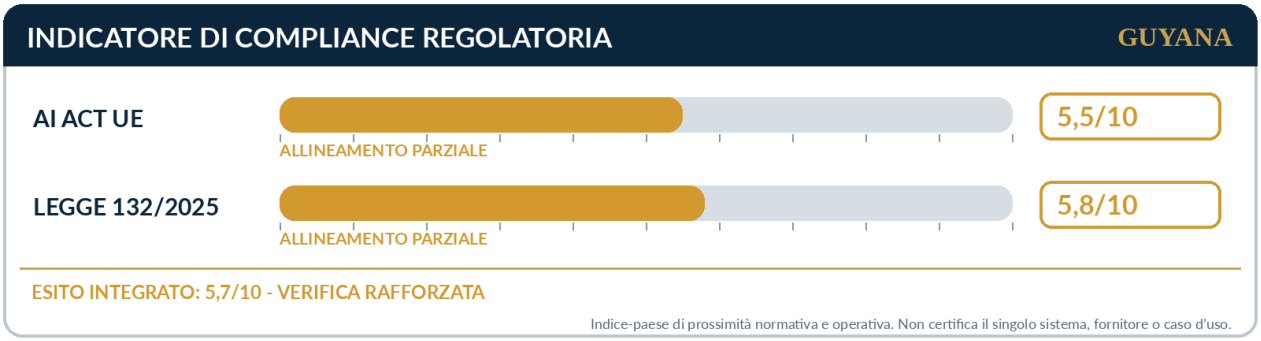
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Guinea-Bissau: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Guyana

Posizione FOTR	77	Area	Americhe	Subregione	America meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,9	GCRI / 10	4,8	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Guyana, AI Act UE 5,5/10; legge 132/2025 5,8/10; esito integrato 5,7/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Guyana è stato membro delle nazioni unite collocato in America meridionale. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 74/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,9/10) supera il GCRI tecnico (4,8/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il quadro di Guyana è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	83,0% / 12,9 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	93,0% / 176 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	54,4 / 37,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	47,2/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	25,6/100 - rank 146	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (74/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,5 / 4,2 / 5,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Guyana, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Guyana le evidenze principali sono GTMI 37,9/100, EGDI 54,4/100, GCI 47,2/100, AI readiness 25,6/100. La dimensione più robusta è maturità infrastrutturale (6,6/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,0/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Guyana è 6,6/10. La base statistica rileva utenti Internet pari al 83,0% nel 2024; 12,9 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 93,0% nel 2024; 176 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Guyana al posto 146 con un valore medio di 25,6/100; il pilastro migliore è governance (39,3/100), quello più debole è sviluppo e diffusione (12,3/100). Il GTMI 2025 è 37,9/100. Il punteggio S2 è 3,0/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Guyana è valutata fragile, con S3 pari a 4,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 59,3/100, sviluppo e diffusione dell'IA 12,3/100, penetrazione Internet 83,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Guyana ottiene S4 5,0/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Guyana, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=5,0/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Guyana è S5 5,1/10. La base ITU registra ITU GCI 47,2/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è organizzazione (5,9/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (74/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,5	Crimini finanziari	8,0
Reti criminali	5,0	Attori incorporati nello Stato	8,0
Attori stranieri	7,0	Attori del settore privato	8,0
Resilienza complessiva	4,2	Cooperazione internazionale	5,5
Politiche e norme nazionali	3,5	Forze dell'ordine	3,5
Antiriciclaggio	4,5	Prevenzione	5,0
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	5,4 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Guyana il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,4/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 2,5/10; le frodi e i reati finanziari 8,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e attori del settore privato (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Guyana assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Guyana, la resilienza complessiva è debole (4,2/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono deboli (3,5/10) e la capacità delle forze dell'ordine è debole (3,5/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 5,0/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Guyana, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Guyana. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Guyana, In Guyana le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Guyana, Il livello governativo di Guyana presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Guyana, Sul piano militare e dual-use, Guyana mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Guyana, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Guyana, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,6/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,6	3,0	4,5	5,0	5,1	4,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,8	5,6	6,0	6,4	5,8	5,6

Il GCRI di Guyana è 4,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,9/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,4/10), mentre il più basso è Maturità cyber (5,6/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,9/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Guyana, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Guyana, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Guyana, Dal punto di vista italiano, Guyana rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Guyana è indicata una cooperazione selettiva, coerente con il FOTR di 5,9/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Maturità cyber a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

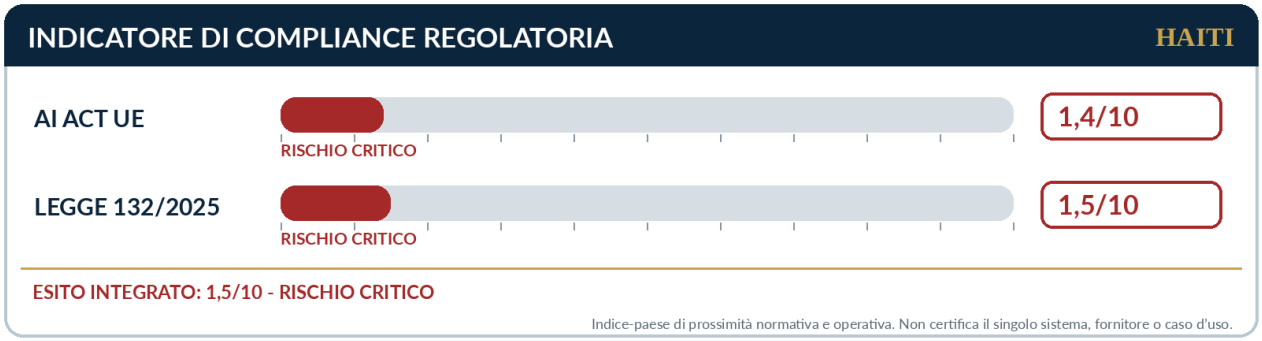
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Guyana: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Haiti

Posizione FOTR	196	Area	Americhe	Subregione	Caraibi
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	1,4	GCRI / 10	1,9	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Haiti, AI Act UE 1,4/10; legge 132/2025 1,5/10; esito integrato 1,5/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Nel quadro di Americhe, Haiti presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 22/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (1,9/10) e indice FOTR (1,4/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Haiti ricade nella fascia di rischio estremo. L'assenza di rimedi affidabili, le restrizioni, l'instabilità o le sanzioni rendono normalmente incompatibile il trattamento locale di dati italiani sensibili o strategici.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	47,9% / 0,3 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	53,9% / 8 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	21,2 / 13,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	24,3/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	15,3/100 - rank 190	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (22/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 2,2 / 6,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Haiti, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Haiti le evidenze principali sono GTMI 13,8/100, EGDI 21,2/100, GCI 24,3/100, AI readiness 15,3/100. La dimensione più robusta è indipendenza della supply chain (2,6/10), mentre la criticità relativa riguarda postura di sicurezza cyber (1,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Haiti è 2,2/10. La base statistica rileva utenti Internet pari al 47,9% nel 2024; 0,3 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 53,9% nel 2024; 8 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Haiti al posto 190 con un valore medio di 15,3/100; il pilastro migliore è resilienza (23,5/100), quello più debole è sviluppo e diffusione (11,1/100). Il GTMI 2025 è 13,8/100. Il punteggio S2 è 1,5/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Haiti è valutata fragile, con S3 pari a 1,9/10. Le evidenze disponibili comprendono indice UN di capitale umano 28,8/100, sviluppo e diffusione dell'IA 11,1/100, penetrazione Internet 47,9%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Haiti ottiene S4 2,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Haiti, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=2,6/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Haiti è S5 1,1/10. La base ITU registra ITU GCI 24,3/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (22/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	8,0
Reti criminali	7,0	Attori incorporati nello Stato	8,5
Attori stranieri	4,5	Attori del settore privato	5,0
Resilienza complessiva	2,2	Cooperazione internazionale	3,5
Politiche e norme nazionali	4,0	Forze dell'ordine	1,5
Antiriciclaggio	2,0	Prevenzione	2,0
Supporto vittime e testimoni	1,5	Rischio operativo FOTR-CY	6,2 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (3,0/10), criminalità finanziaria (8,0/10) e resilienza (2,2/10) colloca Haiti in una fascia di rischio significativo, pari a 6,2/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,5/10) e reti criminali (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Haiti assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Haiti, la resilienza complessiva è molto debole (2,2/10); la cooperazione internazionale è debole (3,5/10), le politiche e norme nazionali sono deboli (4,0/10) e la capacità delle forze dell'ordine è molto debole (1,5/10). Completano il quadro antiriciclaggio 2,0/10, prevenzione 2,0/10 e supporto a vittime e testimoni 1,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Haiti, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Haiti. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Haiti, In Haiti le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Haiti, Il livello governativo di Haiti presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Haiti, Sul piano militare e dual-use, Haiti mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Haiti, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Haiti, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 0,7/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
2,2	1,5	1,9	2,6	1,1	1,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
2,3	0,9	1,0	2,2	0,9	0,7

Il GCRI di Haiti è 1,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 1,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (2,3/10), mentre il più basso è Trasferibilità dati (0,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 1,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Haiti, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Haiti, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Haiti, Dal punto di vista italiano, Haiti rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Haiti, il FOTR di 1,4/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

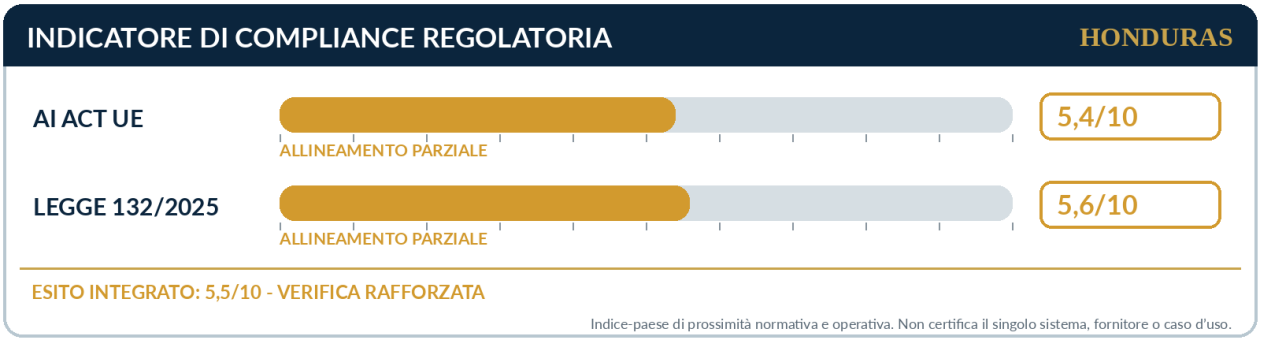
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Haiti: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Honduras

Posizione FOTR	98	Area	Americhe	Subregione	America centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,7	GCRI / 10	4,3	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Honduras, AI Act UE 5,4/10; legge 132/2025 5,6/10; esito integrato 5,5/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Honduras, situato in America centrale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 47/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,7/10) supera il GCRI tecnico (4,3/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il quadro di Honduras è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	58,6% / 4,6 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	95,5% / 149 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	48,6 / 58,1	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	28,1/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	21,7/100 - rank 157	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (47/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,5 / 3,9 / 7,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Honduras, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Honduras le evidenze principali sono GTMI 58,1/100, EGDI 48,6/100, GCI 28,1/100, AI readiness 21,7/100. La dimensione più robusta è indipendenza della supply chain (5,3/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,3/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Honduras è 4,9/10. La base statistica rileva utenti Internet pari al 58,6% nel 2024; 4,6 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 95,5% nel 2024; 149 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Honduras al posto 157 con un valore medio di 21,7/100; il pilastro migliore è governance (38,7/100), quello più debole è politiche pubbliche (4,0/100). Il GTMI 2025 è 58,1/100. Il punteggio S2 è 3,3/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Honduras è valutata fragile, con S3 pari a 4,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 51,8/100, sviluppo e diffusione dell'IA 10,9/100, penetrazione Internet 58,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Honduras ottiene S4 5,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Honduras, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=5,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Honduras è S5 3,8/10. La base ITU registra ITU GCI 28,1/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (47/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,5	Crimini finanziari	7,5
Reti criminali	7,5	Attori incorporati nello Stato	8,5
Attori stranieri	8,0	Attori del settore privato	8,0
Resilienza complessiva	3,9	Cooperazione internazionale	6,0
Politiche e norme nazionali	4,5	Forze dell'ordine	5,0
Antiriciclaggio	4,0	Prevenzione	4,5
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	7,0 - ALTO

Rischio criminale connesso alle tecnologie. In Honduras il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 7,0/10, livello alto. I reati che dipendono direttamente da sistemi informatici raggiungono 6,5/10; le frodi e i reati finanziari 7,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,5/10) e attori stranieri (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Honduras assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Honduras, la resilienza complessiva è debole (3,9/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono deboli (4,5/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 4,5/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Honduras, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Honduras. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Honduras, In Honduras le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Honduras, Il livello governativo di Honduras presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Honduras, Sul piano militare e dual-use, Honduras mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Honduras, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Honduras, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,3/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
4,9	3,3	4,0	5,3	3,8	4,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,0	5,6	5,4	5,9	5,9	5,3

Il GCRI di Honduras è 4,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (6,0/10), mentre il più basso è Trasferibilità dati (5,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Honduras, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Honduras, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Honduras, Dal punto di vista italiano, Honduras rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Honduras è indicata una cooperazione selettiva, coerente con il FOTR di 5,7/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasferibilità dati a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

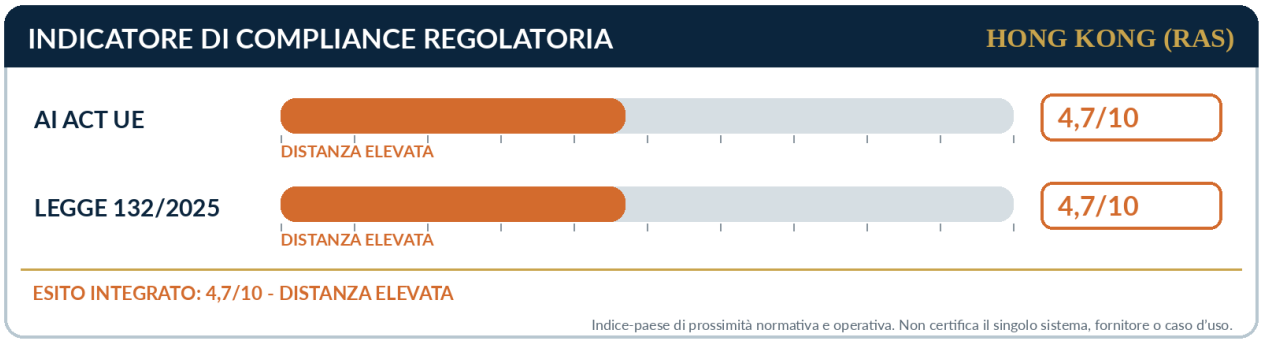
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Honduras: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Hong Kong (RAS)

Posizione FOTR	140	Area	Asia	Subregione	Asia orientale
Status	Regione amministrativa speciale della Cina	Confidenza Celeborn Intelligence	Media	Copertura dati	4/7 famiglie
FOTR / 10	4,6	GCRI / 10	6,0	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Hong Kong (RAS), AI Act UE 4,7/10; legge 132/2025 4,7/10; esito integrato 4,7/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Per un operatore italiano, Hong Kong (RAS) non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 41/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (6,0/10) è superiore al punteggio FOTR (4,6/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Piazza finanziaria e digitale sofisticata, ma progressivamente integrata nel quadro di sicurezza e accesso ai dati della Repubblica Popolare Cinese.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	95,8% / 40,3 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 156.139 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	n.d. / 65,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	n.d./100 - n.d.	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	n.d./100 - rank n.d.	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (41/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	8,0 / 6,2 / 6,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Hong Kong (RAS), n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 4/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Hong Kong (RAS) le evidenze principali sono GTMI 65,2/100. La dimensione più robusta è maturità infrastrutturale (9,8/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (2,9/10). Sono disponibili 4 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata media. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Hong Kong (RAS) è 9,8/10. La base statistica rileva utenti Internet pari al 95,8% nel 2024; 40,3 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 156.139 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Per Hong Kong (RAS) non è disponibile un profilo Oxford Insights direttamente attribuibile; l'adozione di IA è quindi valutata attraverso GovTech, servizi online, infrastrutture e fonti qualitative. Il GTMI 2025 è 65,2/100. Il punteggio S2 è 6,5/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Hong Kong (RAS) è valutata fragile, con S3 pari a 2,9/10. Le evidenze disponibili comprendono penetrazione Internet 95,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Hong Kong (RAS) ottiene S4 5,5/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Hong Kong (RAS), Mercato internazionale ancora ampio, ma con crescente integrazione in fornitori e piattaforme della Cina continentale. L'impatto sulla valutazione è misurato da S4=5,5/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Hong Kong (RAS) è S5 5,1/10. La base ITU registra GCI non disponibile in forma comparabile. Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (41/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Personal Data (Privacy) Ordinance e regole locali, nel contesto della sovranità cinese e della normativa di sicurezza nazionale; necessaria valutazione degli accessi governativi e dei trasferimenti successivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	8,0	Crimini finanziari	7,2
Reti criminali	7,0	Attori incorporati nello Stato	5,5
Attori stranieri	3,0	Attori del settore privato	6,3
Resilienza complessiva	6,2	Cooperazione internazionale	7,1
Politiche e norme nazionali	7,4	Forze dell'ordine	6,7
Antiriciclaggio	6,8	Prevenzione	6,4
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	6,1 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Hong Kong (RAS) presenta un'esposizione stimata significativa (6,1/10): reati cyber-dipendenti 8,0/10, crimini finanziari 7,2/10 e resilienza 6,2/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (7,0/10) e attori del settore privato (6,3/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Hong Kong (RAS) assumono particolare rilevanza compromissioni della supply chain, sottrazione di proprietà intellettuale, furto di cripto-attività, phishing mirato, abuso di identità digitali e intrusioni persistenti contro industria e amministrazioni. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Hong Kong (RAS), la resilienza complessiva è intermedia (6,2/10); la cooperazione internazionale è intermedia (7,1/10), le politiche e norme nazionali sono intermedie (7,4/10) e la capacità delle forze dell'ordine è intermedia (6,7/10). Completano il quadro antiriciclaggio 6,8/10, prevenzione 6,4/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Hong Kong (RAS), il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori. Poiché l'entità non dispone di una serie nazionale GI-TOC autonoma, i valori derivano da un proxy Celeborn Intelligence ponderato su Cina 70%, Singapore 20%, Regno Unito 10%; la confidenza deve pertanto essere considerata inferiore e la decisione resa più prudente.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; proxy Celeborn Intelligence ponderato su Cina 70%, Singapore 20%, Regno Unito 10%. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Hong Kong (RAS), In Hong Kong (RAS) le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Hong Kong (RAS), Il livello governativo di Hong Kong (RAS) presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Hong Kong (RAS), Sul piano militare e dual-use, Hong Kong (RAS) mostra forte ruolo statale e integrazione con filiere cinesi o nazionali, con limitata trasparenza esterna. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Hong Kong (RAS), Personal Data (Privacy) Ordinance e regole locali, nel contesto della sovranità cinese e della normativa di sicurezza nazionale; necessaria valutazione degli accessi governativi e dei trasferimenti successivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Hong Kong (RAS), Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 3,7/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,8	6,5	2,9	5,5	5,1	6,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,6	6,3	2,9	4,6	5,6	3,7

Il GCRI di Hong Kong (RAS) è 6,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (6,3/10), mentre il più basso è Trasparenza istituzionale (2,9/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Hong Kong (RAS), 5 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Hong Kong (RAS), sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Hong Kong (RAS), Dal punto di vista italiano, Hong Kong (RAS) rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Hong Kong (RAS) ricade nella fascia di alto rischio (4,6/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

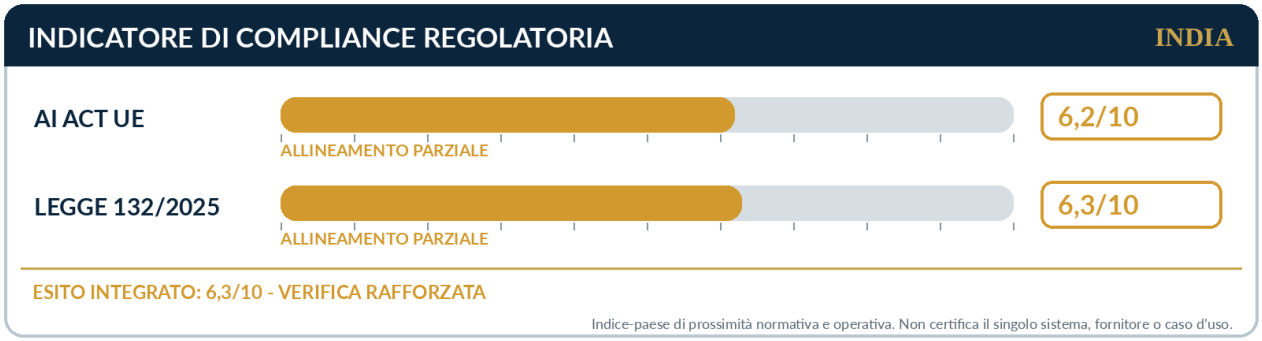
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Hong Kong (RAS): World Development Indicators, valori più recenti disponibili 2022-2024; World Bank GovTech Maturity Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Media con copertura 4/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

India

Posizione FOTR	65	Area	Asia	Subregione	Asia meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	6,2	GCRI / 10	6,7	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di India, AI Act UE 6,2/10; legge 132/2025 6,3/10; esito integrato 6,3/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

L'India è un grande mercato digitale, una potenza software e un polo crescente per data center, semiconduttori, spazio e intelligenza artificiale. La scala federale, le differenze tra Stati, la localizzazione dei dati in alcuni settori e la compresenza di fornitori occidentali, nazionali, giapponesi e asiatici rendono insufficiente una valutazione uniforme. Per l'Italia è un partner strategico, ma ogni progetto deve essere qualificato per settore, Stato federato, operatore e catena di subfornitura. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 62/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,7/10) e indice FOTR (6,2/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Mercato digitale vastissimo, capacità software e servizi globali; la rapida evoluzione normativa e le regole settoriali richiedono una mappatura puntuale dei dati e dei fornitori.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	70,0% / 3,2 per 100	2025/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	99,9% / 1.212 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	66,8 / 96,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	98,5/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	69,5/100 - rank 27	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	51/100 - Parzialmente libero / Parzialmente libero (62/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,5 / 5,5 / 6,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di India, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per India le evidenze principali sono GTMI 96,9/100, EGDI 66,8/100, GCI 98,5/100, AI readiness 69,5/100. La dimensione più robusta è postura di sicurezza cyber (7,9/10), mentre la criticità relativa riguarda maturità infrastrutturale (5,7/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di India è 5,7/10. La base statistica rileva utenti Internet pari al 70,0% nel 2025; 3,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 99,9% nel 2024; 1.212 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca India al posto 27 con un valore medio di 69,5/100; il pilastro migliore è politiche pubbliche (96,0/100), quello più debole è sviluppo e diffusione (54,9/100). Il GTMI 2025 è 96,9/100. Il punteggio S2 è 7,6/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di India è valutata sufficiente ma disomogenea, con S3 pari a 6,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 61,5/100, sviluppo e diffusione dell'IA 54,9/100, penetrazione Internet 70,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di India ottiene S4 6,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di India, Ampia capacità domestica nei servizi e nel software; hardware e telecomunicazioni provenienti da Stati Uniti, Europa, Asia orientale e produttori locali. L'impatto sulla valutazione è misurato

da S4=6,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di India è S5 7,9/10. La base ITU registra ITU GCI 98,5/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è organizzazione (18,5/20). Freedom on the Net è 51/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (62/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Digital Personal Data Protection Act 2023, Information Technology Act e regole settoriali; attuazione progressiva, localizzazione in alcuni comparti e regime di accesso pubblico da valutare.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,5	Crimini finanziari	7,5
Reti criminali	6,5	Attori incorporati nello Stato	7,0
Attori stranieri	3,5	Attori del settore privato	5,0
Resilienza complessiva	5,5	Cooperazione internazionale	8,5
Politiche e norme nazionali	5,5	Forze dell'ordine	5,5
Antiriciclaggio	6,5	Prevenzione	5,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	6,2 - SIGNIFICATIVO

Sintesi del rischio cybercrime. India presenta un'esposizione stimata significativa (6,2/10): reati cyber-dipendenti 7,5/10, crimini finanziari 7,5/10 e resilienza 5,5/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,0/10) e reti criminali (6,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di India assumono particolare rilevanza compromissione delle caselle di posta aziendale, frodi da call center, abuso di portafogli digitali mobili, identità sintetiche, ransomware, phishing bancario e triangolazioni transfrontaliere dei proventi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di India, la resilienza complessiva è debole (5,5/10); la cooperazione internazionale è robusta (8,5/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 6,5/10, prevenzione 5,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in India, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di India. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per India, In India le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per India, Il livello governativo di India presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per India, Sul piano militare e dual-use, India mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per India, Digital Personal Data Protection Act 2023, Information Technology Act e regole settoriali; attuazione progressiva, localizzazione in alcuni comparti e regime di accesso pubblico da valutare. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso India, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,2/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
5,7	7,6	6,0	6,1	7,9	6,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,0	6,6	6,2	6,3	6,7	5,2

Il GCRI di India è 6,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Supply chain (6,7/10), mentre il più basso è Trasferibilità dati (5,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per India, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con India, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e India, Dal punto di vista italiano, India rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per India è indicata una cooperazione selettiva, coerente con il FOTR di 6,2/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasferibilità dati a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

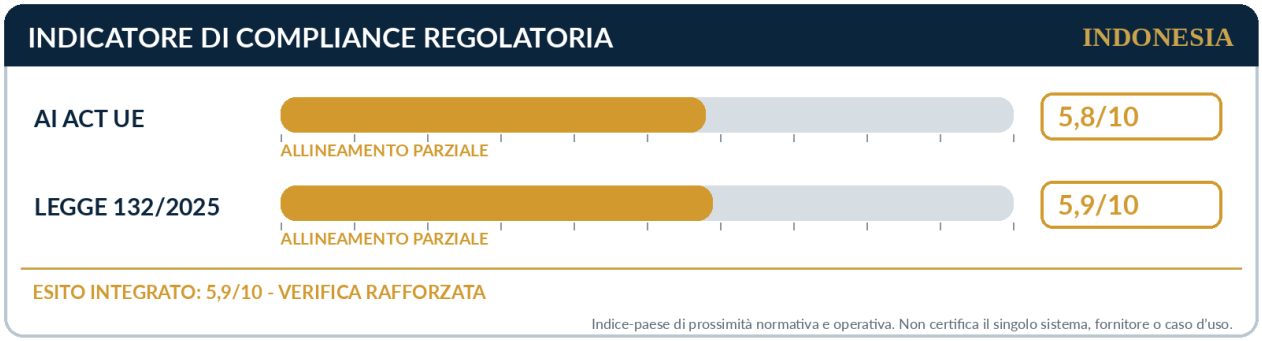
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di India: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Indonesia

Posizione FOTR	86	Area	Asia	Subregione	Asia sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,8	GCRI / 10	6,7	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Indonesia, AI Act UE 5,8/10; legge 132/2025 5,9/10; esito integrato 5,9/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Asia, Indonesia presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La partecipazione al coordinamento BRICS segnala una strategia di autonomia e diversificazione rispetto agli ecosistemi occidentali, con relazioni tecnologiche più intense verso Cina, Russia o altri poli emergenti. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 56/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,7/10) e indice FOTR (5,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Indonesia dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	72,8% / 4,9 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	99,9% / 2.939 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	79,9 / 84,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	100,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	62,4/100 - rank 46	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	48/100 - Parzialmente libero / Parzialmente libero (56/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,5 / 4,3 / 7,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Indonesia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Indonesia le evidenze principali sono GTMI 84,0/100, EGDI 79,9/100, GCI 100,0/100, AI readiness 62,4/100. La dimensione più robusta è postura di sicurezza cyber (7,8/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,7/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Indonesia è 6,9/10. La base statistica rileva utenti Internet pari al 72,8% nel 2024; 4,9 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 99,9% nel 2024; 2.939 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Indonesia al posto 46 con un valore medio di 62,4/100; il pilastro migliore è politiche pubbliche (77,0/100), quello più debole è sviluppo e diffusione (44,1/100). Il GTMI 2025 è 84,0/100. Il punteggio S2 è 6,9/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Indonesia è valutata sufficiente ma disomogenea, con S3 pari a 6,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 72,9/100, sviluppo e diffusione dell'IA 44,1/100, penetrazione Internet 72,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Indonesia ottiene S4 5,7/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Indonesia, Fornitura multi-origine, con forte presenza cinese e statunitense e crescente capacità nazionale. L'impatto sulla valutazione è misurato da S4=5,7/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Indonesia è S5 7,8/10. La base ITU registra ITU GCI 100,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure giuridiche (20,0/20). Freedom on the Net è 48/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (56/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Personal Data Protection Law 27/2022, normativa sui sistemi elettronici e obblighi settoriali; attuazione e vigilanza ancora in consolidamento.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,5	Crimini finanziari	8,0
Reti criminali	7,5	Attori incorporati nello Stato	8,0
Attori stranieri	6,0	Attori del settore privato	8,0
Resilienza complessiva	4,3	Cooperazione internazionale	6,0
Politiche e norme nazionali	5,0	Forze dell'ordine	4,0
Antiriciclaggio	5,0	Prevenzione	4,0
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	7,0 - ALTO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (7,5/10), criminalità finanziaria (8,0/10) e resilienza (4,3/10) colloca Indonesia in una fascia di rischio alto, pari a 7,0/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e attori del settore privato (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Indonesia assumono particolare rilevanza centri organizzati di truffa, frodi d'investimento e sentimentali, phishing multicanale, batterie di schede SIM, conti prestanome, riciclaggio in cripto-attività e compromissione di servizi esternalizzati. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Indonesia, la resilienza complessiva è debole (4,3/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Indonesia, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; controllo della filiera contro esposizione a complessi organizzati per truffe telematiche, call center coercitivi e conti prestanome; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Indonesia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Indonesia, In Indonesia le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Indonesia, Il livello governativo di Indonesia presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Indonesia, Sul piano militare e dual-use, Indonesia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Indonesia, Personal Data Protection Law 27/2022, normativa sui sistemi elettronici e obblighi settoriali; attuazione e vigilanza ancora in consolidamento. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Indonesia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,7/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,9	6,9	6,2	5,7	7,8	6,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,7	6,5	5,5	6,2	6,1	4,7

Il GCRI di Indonesia è 6,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (6,5/10), mentre il più basso è Trasferibilità dati (4,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Indonesia, 1 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Indonesia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Indonesia, Dal punto di vista italiano, Indonesia rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Indonesia è indicata una cooperazione selettiva, coerente con il FOTR di 5,8/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

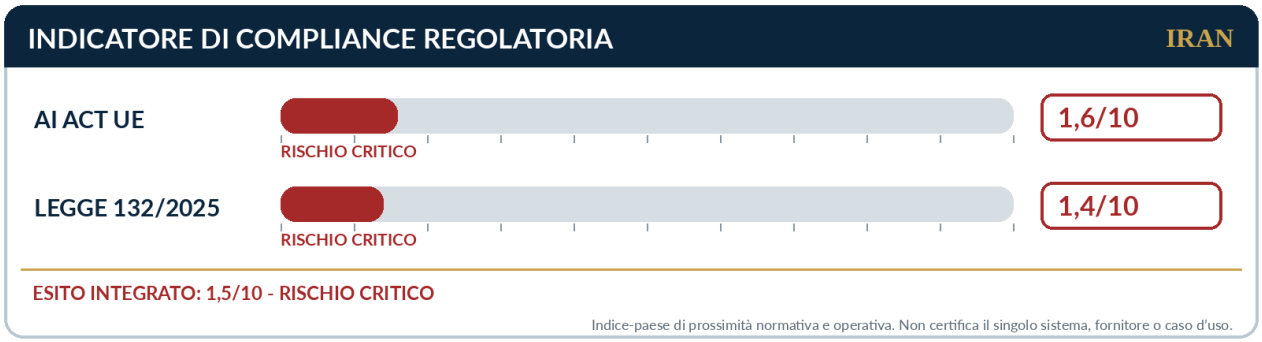
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Indonesia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Iran

Posizione FOTR	200	Area	Asia	Subregione	Medio Oriente e Asia occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	1,2	GCRI / 10	5,3	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Iran, AI Act UE 1,6/10; legge 132/2025 1,4/10; esito integrato 1,5/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

L'Iran possiede competenze scientifiche, industriali e cyber significative, sviluppate anche in risposta a sanzioni e isolamento tecnologico. Il controllo pubblico delle comunicazioni, la frammentazione di Internet, il contesto sanzionatorio e la dimensione militare delle tecnologie producono tuttavia un livello di rischio elevato per dati, proprietà intellettuale e continuità. Ogni rapporto italiano deve partire da screening legale e autorizzativo, non dalla sola qualità tecnica del partner. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 10/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (5,3/10) è superiore al punteggio FOTR (1,2/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Per Iran la regola operativa è evitare trasferimenti e dipendenze tecnologiche, salvo finalità umanitarie o istituzionali autorizzate e protette da architetture isolate. Il contratto, da solo, non rende il rischio accettabile.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	85,3% / 12,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 7.226 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	65,6 / 68,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	65,5/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	51,0/100 - rank 76	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	13/100 - Non libero / Non libero (10/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	8,5 / 3,1 / 8,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Iran, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Iran le evidenze principali sono GTMI 68,6/100, EGDI 65,6/100, GCI 65,5/100, AI readiness 51,0/100. La dimensione più robusta è maturità infrastrutturale (7,8/10), mentre la criticità relativa riguarda postura di sicurezza cyber (4,2/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Iran è 7,8/10. La base statistica rileva utenti Internet pari al 85,3% nel 2024; 12,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 7.226 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Iran al posto 76 con un valore medio di 51,0/100; il pilastro migliore è politiche pubbliche (84,5/100), quello più debole è sviluppo e diffusione (37,6/100). Il GTMI 2025 è 68,6/100. Il punteggio S2 è 5,3/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Iran è valutata fragile, con S3 pari a 4,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 69,3/100, sviluppo e diffusione dell'IA 37,6/100, penetrazione Internet 85,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Iran ottiene S4 4,3/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina, Russia; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Iran, Capacità domestiche e forniture cinesi/russe; accesso limitato a tecnologie occidentali per effetto delle sanzioni. L'impatto sulla valutazione è misurato da S4=4,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Iran è S5 4,2/10. La base ITU registra ITU GCI 65,5/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è cooperazione (6,2/20). Freedom on the Net è 13/100 - Non libero, mentre Freedom in the World è Non libero (10/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa frammentata, controlli estesi sulle comunicazioni e regime sanzionatorio internazionale; localizzazione, accessi pubblici e continuità operativa rendono estremamente problematici i trasferimenti.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	8,5	Crimini finanziari	9,0
Reti criminali	7,5	Attori incorporati nello Stato	9,5
Attori stranieri	5,5	Attori del settore privato	5,0
Resilienza complessiva	3,1	Cooperazione internazionale	4,0
Politiche e norme nazionali	4,0	Forze dell'ordine	3,0
Antiriciclaggio	2,5	Prevenzione	3,0
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	8,1 - CRITICO

Quadro criminale digitale. Per Iran, l'indice operativo FOTR-CY è 8,1/10, classe critica. Il mercato dei reati cyber-dipendenti è molto elevato (8,5/10), mentre i crimini finanziari sono molto elevati (9,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,5/10) e reti criminali (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Iran assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Iran, la resilienza complessiva è molto debole (3,1/10); la cooperazione internazionale è debole (4,0/10), le politiche e norme nazionali sono deboli (4,0/10) e la capacità delle forze dell'ordine è molto debole (3,0/10). Completano il quadro antiriciclaggio 2,5/10, prevenzione 3,0/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Iran, il livello critico non determina da solo un divieto, ma modifica il perimetro accettabile: assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Iran. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Iran, In Iran le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Iran, Il livello governativo di Iran presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Iran, Sul piano militare e dual-use, Iran mostra capacità domestiche e cooperazione con partner soggetti a sanzioni o restrizioni. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Iran, Normativa frammentata, controlli estesi sulle comunicazioni e regime sanzionatorio internazionale; localizzazione, accessi pubblici e continuità operativa rendono estremamente problematici i trasferimenti. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Iran, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 0,0/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,8	5,3	4,8	4,3	4,2	5,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
1,2	3,5	0,3	0,0	2,3	0,0

Il GCRI di Iran è 5,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 1,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (3,5/10), mentre il più basso è Compatibilità strategica (0,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 1,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Iran, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Iran, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Iran, Dal punto di vista italiano, Iran rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Iran, il FOTR di 1,2/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

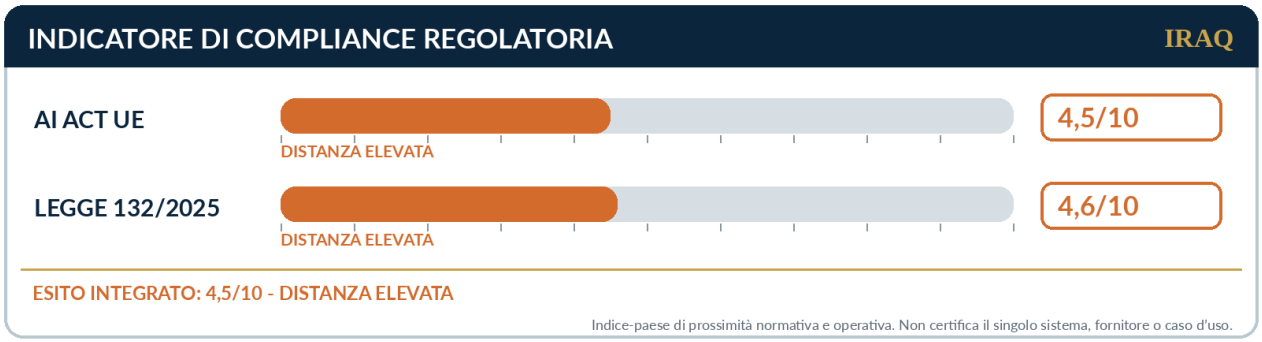
Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.
Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.
Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Iran: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Iraq

Posizione FOTR	**141**	**Area**	Asia	**Subregione**	Medio Oriente e Asia occidentale
Status	**Stato membro delle Nazioni Unite**	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	7/7 famiglie
FOTR / 10	**4,6**	**GCRI / 10**	**4,3**	**Classe operativa**	**Rischio alto**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Iraq, AI Act UE 4,5/10; legge 132/2025 4,6/10; esito integrato 4,5/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Per un operatore italiano, Iraq non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 31/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (4,3/10) e indice FOTR (4,6/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Iraq presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	81,5% / 17,6 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 35 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	45,7 / 46,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	53,1/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	29,4/100 - rank 128	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	41/100 - Parzialmente libero / Non libero (31/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 3,3 / 6,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Iraq, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Iraq le evidenze principali sono GTMI 46,4/100, EGDI 45,7/100, GCI 53,1/100, AI readiness 29,4/100. La dimensione più robusta è maturità infrastrutturale (6,2/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,2/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Iraq è 6,2/10. La base statistica rileva utenti Internet pari al 81,5% nel 2024; 17,6 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 35 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Iraq al posto 128 con un valore medio di 29,4/100; il pilastro migliore è resilienza (42,6/100), quello più debole è adozione pubblica (5,3/100). Il GTMI 2025 è 46,4/100. Il punteggio S2 è 3,2/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Iraq è valutata fragile, con S3 pari a 4,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 49,7/100, sviluppo e diffusione dell'IA 35,0/100, penetrazione Internet 81,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Iraq ottiene S4 4,0/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Iraq, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo societario e

subfornitura. L'impatto sulla valutazione è misurato da S4=4,0/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Iraq è S5 4,0/10. La base ITU registra ITU GCI 53,1/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è cooperazione (8,1/20). Freedom on the Net è 41/100 - Parzialmente libero, mentre Freedom in the World è Non libero (31/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	9,0
Reti criminali	8,0	Attori incorporati nello Stato	8,5
Attori stranieri	9,0	Attori del settore privato	7,5
Resilienza complessiva	3,3	Cooperazione internazionale	4,5
Politiche e norme nazionali	3,5	Forze dell'ordine	3,5
Antiriciclaggio	4,0	Prevenzione	3,0
Supporto vittime e testimoni	2,5	Rischio operativo FOTR-CY	6,5 - ALTO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (3,0/10), criminalità finanziaria (9,0/10) e resilienza (3,3/10) colloca Iraq in una fascia di rischio alto, pari a 6,5/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (9,0/10) e attori incorporati nello Stato (8,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Iraq assumono particolare rilevanza phishing e credential theft, ransomware, frodi d'investimento, attacchi a energia e servizi pubblici, abuso di cripto-attività e campagne che possono combinare profitto, spionaggio e pressione politica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Iraq, la resilienza complessiva è molto debole (3,3/10); la cooperazione internazionale è debole (4,5/10), le politiche e norme nazionali sono deboli (3,5/10) e la capacità delle forze dell'ordine è debole (3,5/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 3,0/10 e supporto a vittime e testimoni 2,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Iraq, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Iraq. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Iraq, In Iraq le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Iraq, Il livello governativo di Iraq presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Iraq, Sul piano militare e dual-use, Iraq mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Iraq, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Iraq, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 4,0/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,2	3,2	4,1	4,0	4,0	4,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,1	4,6	4,2	5,1	4,5	4,0

Il GCRI di Iraq è 4,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (5,1/10), mentre il più basso è Trasferibilità dati (4,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Iraq, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Iraq, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Iraq, Dal punto di vista italiano, Iraq rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Iraq ricade nella fascia di alto rischio (4,6/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

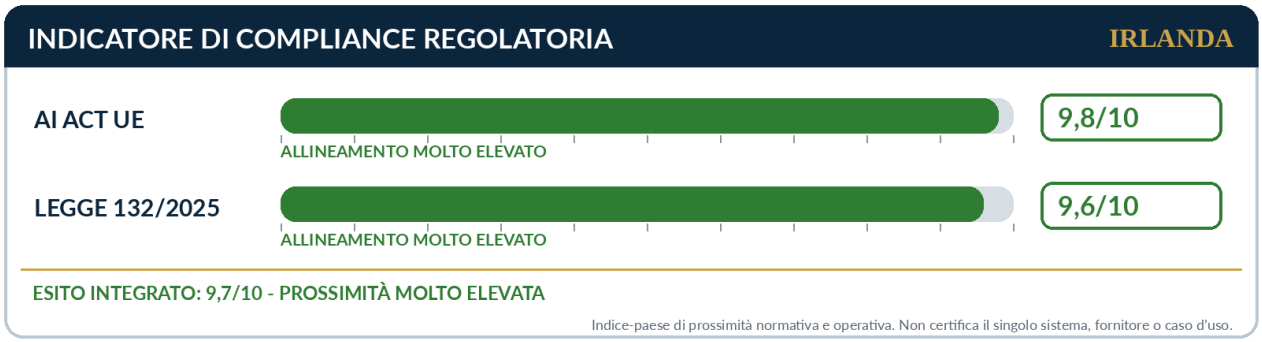
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Iraq: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Irlanda

Posizione FOTR	17	Area	Europa	Subregione	Europa occidentale e centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,9	GCRI / 10	8,1	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Irlanda, AI Act UE 9,8/10; legge 132/2025 9,6/10; esito integrato 9,7/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Irlanda è stato membro delle nazioni unite collocato in Europa occidentale e centrale. L'appartenenza all'Unione europea inserisce il Paese nel mercato digitale unico, nel sistema GDPR e nelle principali discipline comuni su cybersicurezza, dati e intelligenza artificiale. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 98/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,1/10) e indice FOTR (8,9/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Irlanda presenta un ecosistema digitale maturo, istituzioni generalmente prevedibili e una buona capacità di gestione degli incidenti. Il rischio residuo deriva soprattutto dalla concentrazione cloud, dalle dipendenze extraeuropee e dalla complessità delle filiere software.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	97,2% / 32,3 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 121.468 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	91,4 / 89,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	90,9/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	73,2/100 - rank 17	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (98/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Firmatario/invitato	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,0 / 7,4 / 4,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Irlanda, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Irlanda le evidenze principali sono GTMI 89,7/100, EGDI 91,4/100, GCI 90,9/100, AI readiness 73,2/100. La dimensione più robusta è maturità infrastrutturale (9,4/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,4/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Irlanda è 9,4/10. La base statistica rileva utenti Internet pari al 97,2% nel 2024; 32,3 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 121.468 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Irlanda al posto 17 con un valore medio di 73,2/100; il pilastro migliore è governance (94,6/100), quello più debole è sviluppo e diffusione (56,9/100). Il GTMI 2025 è 89,7/100. Il punteggio S2 è 7,7/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Irlanda è valutata solida, con S3 pari a 8,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 90,5/100, sviluppo e diffusione dell'IA 56,9/100, penetrazione Internet 97,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Irlanda ottiene S4 6,4/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Irlanda, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,4/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Irlanda è S5 8,7/10. La base ITU registra ITU GCI 90,9/100, Tier 2 - avanzato; il pilastro relativamente più debole è misure tecniche (13,5/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (98/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Firmatario/invitato. Quadro normativo sintetico: GDPR, Data Protection Act 2018, NIS2 e corpus digitale UE; ruolo centrale per molti fornitori cloud e piattaforme stabiliti nell'Unione.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,0	Crimini finanziari	6,0
Reti criminali	5,5	Attori incorporati nello Stato	4,0
Attori stranieri	5,5	Attori del settore privato	3,0
Resilienza complessiva	7,4	Cooperazione internazionale	8,0
Politiche e norme nazionali	8,0	Forze dell'ordine	7,5
Antiriciclaggio	7,5	Prevenzione	6,0
Supporto vittime e testimoni	7,5	Rischio operativo FOTR-CY	4,8 - MODERATO

Rischio criminale connesso alle tecnologie. In Irlanda il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 4,8/10, livello moderato. I reati che dipendono direttamente da sistemi informatici raggiungono 6,0/10; le frodi e i reati finanziari 6,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (5,5/10) e attori stranieri (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Irlanda assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Irlanda, la resilienza complessiva è intermedia (7,4/10); la cooperazione internazionale è robusta (8,0/10), le politiche e norme nazionali sono robuste (8,0/10) e la capacità delle forze dell'ordine è robusta (7,5/10). Completano il quadro antiriciclaggio 7,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 7,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Irlanda, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Irlanda. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Irlanda, In Irlanda le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Irlanda, Il livello governativo di Irlanda presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Irlanda, Sul piano militare e dual-use, Irlanda mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Irlanda, GDPR, Data Protection Act 2018, NIS2 e corpus digitale UE; ruolo centrale per molti fornitori cloud e piattaforme stabiliti nell'Unione. Lo stato rispetto alla Convenzione di Budapest è: Firmatario/invitato; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Irlanda, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,8/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,4	7,7	8,1	6,4	8,7	8,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,7	8,2	7,9	9,7	8,1	9,8

Il GCRI di Irlanda è 8,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,9/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,8/10), mentre il più basso è Trasparenza istituzionale (7,9/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Basso	Medio-basso	Basso

La matrice applica il FOTR di 8,9/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Irlanda, la cautela si concentra su 1 ambiti a rischio intermedio: Pubblica amministrazione. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Irlanda, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Irlanda, Dal punto di vista italiano, Irlanda rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Irlanda, il FOTR di 8,9/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (7,9/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

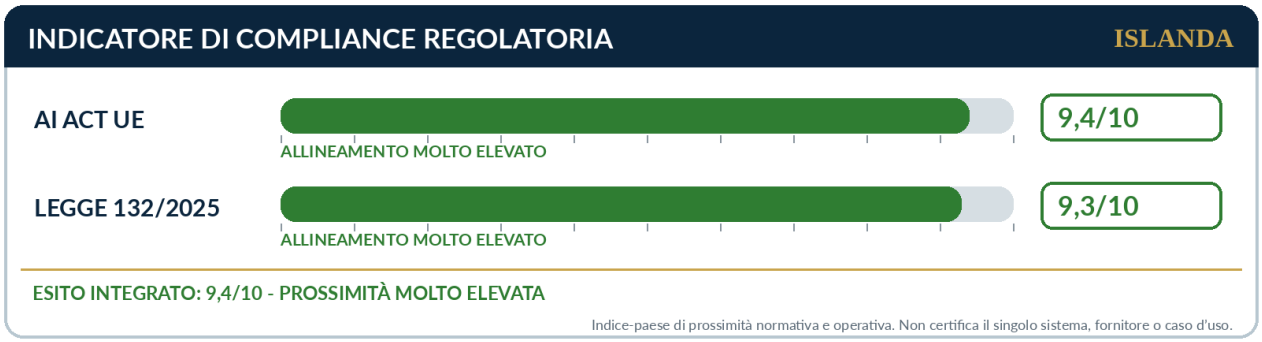
Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Irlanda: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Islanda

Posizione FOTR	**11**	**Area**	Europa	**Subregione**	Europa settentrionale e baltica
Status	**Stato membro delle Nazioni Unite**	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	7/7 famiglie
FOTR / 10	**9,0**	**GCRI / 10**	**8,1**	**Classe operativa**	**Affidabilità molto alta**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Islanda, AI Act UE 9,4/10; legge 132/2025 9,3/10; esito integrato 9,4/10, classe «Allineamento molto elevato». L'integrazione nello Spazio economico europeo riduce la distanza regolatoria, senza eliminare la necessità di verificare autorità competenti, norme settoriali, trasferimenti e catena dei responsabili. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Nel quadro di Europa, Islanda presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La partecipazione allo Spazio economico europeo produce una forte prossimità normativa con l'Italia, pur richiedendo verifiche settoriali e contrattuali. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 95/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,1/10) e indice FOTR (9,0/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il sistema digitale di Islanda è avanzato e integrato con standard internazionali. Le principali criticità non sono di base istituzionale, ma riguardano supply chain, concentrazione dei servizi e gestione delle eccezioni di sicurezza nazionale.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	98,2% / 37,5 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 88.084 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	96,7 / 94,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	99,1/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	64,5/100 - rank 44	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	94/100 - Libero / Libero (95/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 8,2 / 3,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Islanda, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Islanda le evidenze principali sono GTMI 94,8/100, EGDI 96,7/100, GCI 99,1/100, AI readiness 64,5/100. La dimensione più robusta è maturità infrastrutturale (9,8/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,0/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Islanda è 9,8/10. La base statistica rileva utenti Internet pari al 98,2% nel 2024; 37,5 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 88.084 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Islanda al posto 44 con un valore medio di 64,5/100; il pilastro migliore è politiche pubbliche (77,0/100), quello più debole è sviluppo e diffusione (43,0/100). Il GTMI 2025 è 94,8/100. Il punteggio S2 è 7,3/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Islanda è valutata sufficiente ma disomogenea, con S3 pari a 7,9/10. Le evidenze disponibili comprendono indice UN di capitale umano 99,5/100, sviluppo e diffusione dell'IA 43,0/100, penetrazione Internet 98,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Islanda ottiene S4 6,0/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Islanda, Fornitura prevalentemente nazionale, europea e statunitense, con catene hardware globali. In genere è possibile diversificare e imporre requisiti contrattuali elevati. L'impatto sulla valutazione è

misurato da S4=6,0/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Islanda è S5 9,5/10. La base ITU registra ITU GCI 99,1/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è organizzazione (19,4/20). Freedom on the Net è 94/100 - Libero, mentre Freedom in the World è Libero (95/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR incorporato nello SEE, legge nazionale sulla protezione dei dati e disciplina di sicurezza delle reti coerente con il quadro europeo.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	5,0
Reti criminali	4,5	Attori incorporati nello Stato	1,0
Attori stranieri	4,5	Attori del settore privato	2,0
Resilienza complessiva	8,2	Cooperazione internazionale	8,5
Politiche e norme nazionali	8,5	Forze dell'ordine	9,0
Antiriciclaggio	8,0	Prevenzione	8,0
Supporto vittime e testimoni	7,5	Rischio operativo FOTR-CY	3,9 - MODERATO

Pressione del crimine digitale. Il profilo di Islanda restituisce un rischio FOTR-CY di 3,9/10 (moderato). La componente cyber-dipendente vale 5,5/10 e quella finanziaria 5,0/10; la risposta sistemica è valutata robusta, con resilienza media di 8,2/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (4,5/10) e attori stranieri (4,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Islanda assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Islanda, la resilienza complessiva è robusta (8,2/10); la cooperazione internazionale è robusta (8,5/10), le politiche e norme nazionali sono robuste (8,5/10) e la capacità delle forze dell'ordine è robusta (9,0/10). Completano il quadro antiriciclaggio 8,0/10, prevenzione 8,0/10 e supporto a vittime e testimoni 7,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Islanda, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Islanda. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Islanda, In Islanda le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Islanda, Il livello governativo di Islanda presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Islanda, Sul piano militare e dual-use, Islanda mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Islanda, GDPR incorporato nello SEE, legge nazionale sulla protezione dei dati e disciplina di sicurezza delle reti coerente con il quadro europeo. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Islanda, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,5/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,8	7,3	7,9	6,0	9,5	8,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,3	9,0	8,5	9,1	8,4	9,5

Il GCRI di Islanda è 8,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 9,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,5/10), mentre il più basso è Supply chain (8,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Basso	Basso	Basso

La matrice applica il FOTR di 9,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Islanda, la matrice non individua ambiti ad alto rischio; 6 categorie risultano basse o medio-basse, ferma la verifica del singolo progetto. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Islanda, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Islanda, Dal punto di vista italiano, Islanda rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Islanda, il FOTR di 9,0/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (8,4/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

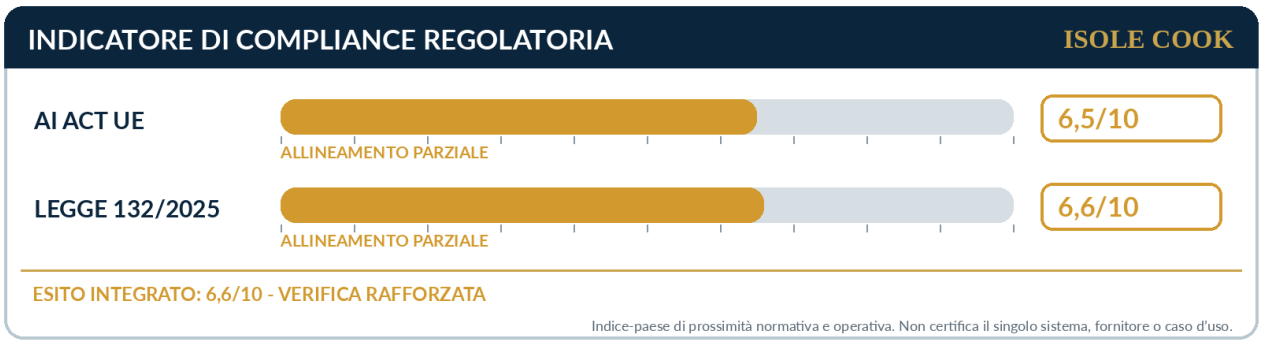
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Islanda: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Isole Cook

Posizione FOTR	57	Area	Oceania	Subregione	Pacifico insulare
Status	Stato autogovernato in libera associazione con la Nuova Zelanda	Confidenza Celeborn Intelligence	Bassa	Copertura dati	0/7 famiglie
FOTR / 10	6,5	GCRI / 10	6,1	Classe operativa	Affidabilità favorevole ma condizionata

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Isole Cook, AI Act UE 6,5/10; legge 132/2025 6,6/10; esito integrato 6,6/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Isole Cook, situato in Pacifico insulare, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La distanza geografica e l'insularità rendono centrali cavi sottomarini, satelliti, continuità energetica e dipendenza da fornitori australiani, neozelandesi, statunitensi o asiatici. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Per questa entità non è disponibile un indicatore Freedom in the World direttamente comparabile; l'assenza di copertura viene trattata come limite informativo e non come prova automatica di rischio. GCRI tecnico (6,1/10) e indice FOTR (6,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. In Isole Cook la trasformazione digitale procede più rapidamente dell'uniformità regolatoria e operativa. Gli investimenti devono essere accompagnati da audit, clausole di uscita e gestione locale del rischio.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	n.d. / n.d. per 100	n.d./n.d.	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	n.d. / n.d. per milione	n.d./n.d.	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	n.d. / n.d.	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	n.d./100 - n.d.	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	n.d./100 - rank n.d.	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / n.d.	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,5 / 7,4 / 5,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Isole Cook, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 0/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Isole Cook le evidenze principali sono nessun indicatore composito pienamente comparabile. La dimensione più robusta è capitale umano e competenze digitali (6,7/10), mentre la criticità relativa riguarda indipendenza della supply chain (4,6/10). Sono disponibili 0 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata bassa. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Isole Cook è 6,3/10. La base statistica rileva i principali dati WDI non sono disponibili in forma omogenea. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Per Isole Cook non è disponibile un profilo Oxford Insights direttamente attribuibile; l'adozione di IA è quindi valutata attraverso GovTech, servizi online, infrastrutture e fonti qualitative. Il punteggio S2 è 6,4/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Isole Cook è valutata sufficiente ma disomogenea, con S3 pari a 6,7/10. Le evidenze disponibili comprendono evidenza quantitativa incompleta. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Isole Cook ottiene S4 4,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Isole Cook, Dipendenza da Australia, Nuova Zelanda, Stati Uniti, Francia e operatori satellitari o sottomarini; la scala ridotta limita la diversificazione e aumenta il rischio di concentrazione. L'impatto sulla valutazione è misurato da S4=4,6/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Isole Cook è S5 6,3/10. La base ITU registra GCI non disponibile in forma comparabile. Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è n.d.. Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,5	Crimini finanziari	6,7
Reti criminali	5,9	Attori incorporati nello Stato	2,4
Attori stranieri	5,2	Attori del settore privato	4,6
Resilienza complessiva	7,4	Cooperazione internazionale	7,9
Politiche e norme nazionali	7,6	Forze dell'ordine	7,0
Antiriciclaggio	6,8	Prevenzione	7,1
Supporto vittime e testimoni	7,5	Rischio operativo FOTR-CY	5,1 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Isole Cook presenta un'esposizione stimata significativa (5,1/10): reati cyber-dipendenti 6,5/10, crimini finanziari 6,7/10 e resilienza 7,4/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (5,9/10) e attori stranieri (5,2/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Isole Cook assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Isole Cook, la resilienza complessiva è intermedia (7,4/10); la cooperazione internazionale è robusta (7,9/10), le politiche e norme nazionali sono robuste (7,6/10) e la capacità delle forze dell'ordine è intermedia (7,0/10). Completano il quadro antiriciclaggio 6,8/10, prevenzione 7,1/10 e supporto a vittime e testimoni 7,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Isole Cook, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova. Poiché l'entità non dispone di una serie nazionale GI-TOC autonoma, i valori derivano da un proxy Celeborn Intelligence ponderato su Nuova Zelanda 80%, Figi 20%; la confidenza deve pertanto essere considerata inferiore e la decisione resa più prudente.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; proxy Celeborn Intelligence ponderato su Nuova Zelanda 80%, Figi 20%. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Isole Cook, In Isole Cook le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Isole Cook, Il livello governativo di Isole Cook presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Isole Cook, Sul piano militare e dual-use, Isole Cook mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Isole Cook, Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Isole Cook, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 6,3/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,3	6,4	6,7	4,6	6,3	6,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,8	6,1	6,7	7,4	5,5	6,3

Il GCRI di Isole Cook è 6,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (7,4/10), mentre il più basso è Supply chain (5,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Isole Cook, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Isole Cook, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Isole Cook, Dal punto di vista italiano, Isole Cook rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Isole Cook è favorevole ma condizionata: il valore FOTR di 6,5/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Supply chain.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

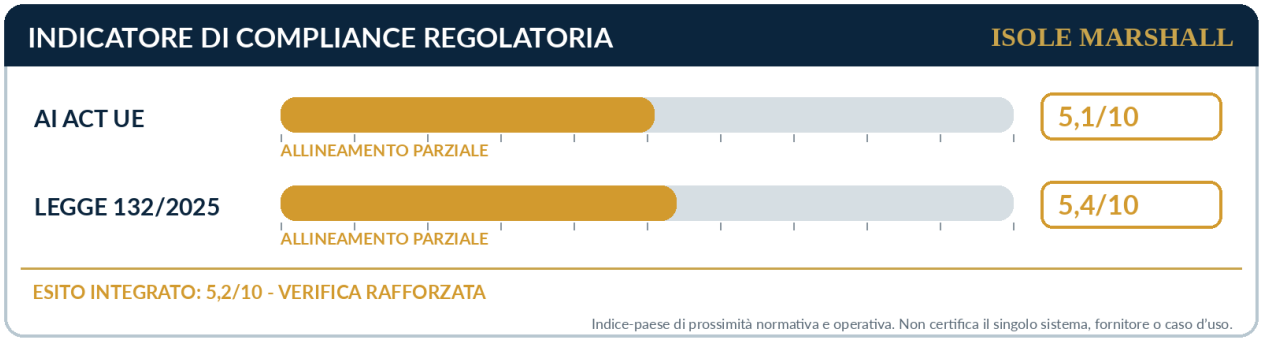
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Isole Cook: World Development Indicators, valori più recenti disponibili 2022-2024; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Bassa con copertura 0/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Isole Marshall

Posizione FOTR	121	Area	Oceania	Subregione	Pacifico insulare
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,4	GCRI / 10	3,6	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Isole Marshall, AI Act UE 5,1/10; legge 132/2025 5,4/10; esito integrato 5,2/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Isole Marshall non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La distanza geografica e l'insularità rendono centrali cavi sottomarini, satelliti, continuità energetica e dipendenza da fornitori australiani, neozelandesi, statunitensi o asiatici. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 93/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,4/10) supera il GCRI tecnico (3,6/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Isole Marshall presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	65,9% / 2,4 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	97,2% / 213 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	48,2 / 12,1	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	14,2/100 - Tier 5 - capacità iniziali	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	16,1/100 - rank 177	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (93/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	1,5 / 5,7 / 2,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Isole Marshall, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Isole Marshall le evidenze principali sono GTMI 12,1/100, EGDI 48,2/100, GCI 14,2/100, AI readiness 16,1/100. La dimensione più robusta è capitale umano e competenze digitali (4,9/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,0/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Isole Marshall è 4,4/10. La base statistica rileva utenti Internet pari al 65,9% nel 2024; 2,4 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 97,2% nel 2024; 213 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Isole Marshall al posto 177 con un valore medio di 16,1/100; il pilastro migliore è infrastrutture IA (40,5/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 12,1/100. Il punteggio S2 è 2,0/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Isole Marshall è valutata fragile, con S3 pari a 4,9/10. Le evidenze disponibili comprendono indice UN di capitale umano 78,4/100, sviluppo e diffusione dell'IA 18,5/100, penetrazione Internet 65,9%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Isole Marshall ottiene S4 3,9/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Isole Marshall, Dipendenza da Australia, Nuova Zelanda, Stati Uniti, Francia e operatori satellitari o sottomarini; la scala ridotta limita la diversificazione e aumenta il rischio di concentrazione. L'impatto sulla

valutazione è misurato da S4=3,9/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Isole Marshall è S5 2,7/10. La base ITU registra ITU GCI 14,2/100, Tier 5 - capacità iniziali; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (93/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	1,5	Crimini finanziari	3,5
Reti criminali	2,5	Attori incorporati nello Stato	2,5
Attori stranieri	3,0	Attori del settore privato	2,0
Resilienza complessiva	5,7	Cooperazione internazionale	6,0
Politiche e norme nazionali	6,0	Forze dell'ordine	5,5
Antiriciclaggio	4,5	Prevenzione	4,5
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	2,9 - CONTENUTO

Pressione del crimine digitale. Il profilo di Isole Marshall restituisce un rischio FOTR-CY di 2,9/10 (contenuto). La componente cyber-dipendente vale 1,5/10 e quella finanziaria 3,5/10; la risposta sistemica è valutata intermedia, con resilienza media di 5,7/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (3,0/10) e reti criminali (2,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Isole Marshall assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Isole Marshall, la resilienza complessiva è intermedia (5,7/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 4,5/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Isole Marshall, il livello contenuto non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Isole Marshall. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Isole Marshall, In Isole Marshall le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Isole Marshall, Il livello governativo di Isole Marshall presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Isole Marshall, Sul piano militare e dual-use, Isole Marshall mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Isole Marshall, Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Isole Marshall, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,4/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
4,4	2,0	4,9	3,9	2,7	3,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,9	4,7	5,6	6,2	4,6	5,4

Il GCRI di Isole Marshall è 3,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,2/10), mentre il più basso è Supply chain (4,6/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio-alto	Medio-alto	Medio-alto	Medio

La matrice applica il FOTR di 5,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Isole Marshall, 3 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Cloud e infrastrutture, IP e R&S, Pubblica amministrazione. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Isole Marshall, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Isole Marshall, Dal punto di vista italiano, Isole Marshall rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Isole Marshall è indicata una cooperazione selettiva, coerente con il FOTR di 5,4/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Cloud e infrastrutture a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

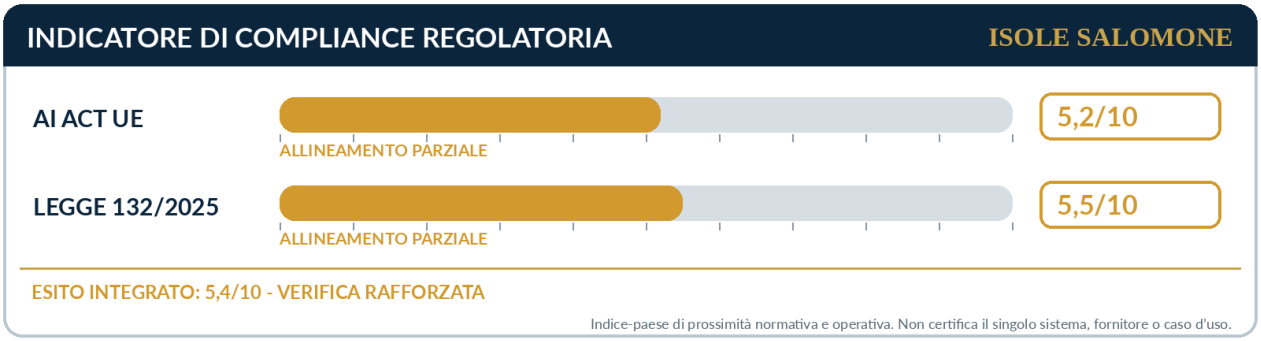
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Isole Marshall: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Isole Salomone

Posizione FOTR	113	Area	Oceania	Subregione	Pacifico insulare
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,5	GCRI / 10	3,2	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Isole Salomone, AI Act UE 5,2/10; legge 132/2025 5,5/10; esito integrato 5,4/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Isole Salomone è stato membro delle nazioni unite collocato in Pacifico insulare. La distanza geografica e l'insularità rendono centrali cavi sottomarini, satelliti, continuità energetica e dipendenza da fornitori australiani, neozelandesi, statunitensi o asiatici. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 74/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,5/10) supera il GCRI tecnico (3,2/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il quadro di Isole Salomone è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	29,0% / 0,1 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	81,5% / 81 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	36,8 / 26,1	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	17,7/100 - Tier 5 - capacità iniziali	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	20,8/100 - rank 162	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (74/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	1,5 / 4,7 / 4,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Isole Salomone, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Isole Salomone le evidenze principali sono GTMI 26,1/100, EGDI 36,8/100, GCI 17,7/100, AI readiness 20,8/100. La dimensione più robusta è indipendenza della supply chain (3,8/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,7/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Isole Salomone è 2,8/10. La base statistica rileva utenti Internet pari al 29,0% nel 2024; 0,1 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 81,5% nel 2024; 81 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Isole Salomone al posto 162 con un valore medio di 20,8/100; il pilastro migliore è infrastrutture IA (33,7/100), quello più debole è politiche pubbliche (4,0/100). Il GTMI 2025 è 26,1/100. Il punteggio S2 è 2,7/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Isole Salomone è valutata fragile, con S3 pari a 3,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 42,6/100, sviluppo e diffusione dell'IA 20,5/100, penetrazione Internet 29,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Isole Salomone ottiene S4 3,8/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Isole Salomone, Dipendenza da Australia, Nuova Zelanda, Stati Uniti, Francia e operatori satellitari o sottomarini; la scala ridotta limita la diversificazione e aumenta il rischio di concentrazione. L'impatto sulla

valutazione è misurato da S4=3,8/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Isole Salomone è S5 3,0/10. La base ITU registra ITU GCI 17,7/100, Tier 5 - capacità iniziali; il pilastro relativamente più debole è sviluppo delle capacità (0,8/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (74/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	1,5	Crimini finanziari	7,0
Reti criminali	4,5	Attori incorporati nello Stato	7,5
Attori stranieri	7,0	Attori del settore privato	7,0
Resilienza complessiva	4,7	Cooperazione internazionale	5,0
Politiche e norme nazionali	4,5	Forze dell'ordine	5,5
Antiriciclaggio	4,0	Prevenzione	6,5
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	4,7 - MODERATO

Quadro criminale digitale. Per Isole Salomone, l'indice operativo FOTR-CY è 4,7/10, classe moderata. Il mercato dei reati cyber-dipendenti è limitato o poco osservabile (1,5/10), mentre i crimini finanziari sono elevati (7,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,5/10) e attori stranieri (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Isole Salomone assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Isole Salomone, la resilienza complessiva è debole (4,7/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono deboli (4,5/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 6,5/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Isole Salomone, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Isole Salomone. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Isole Salomone, In Isole Salomone le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Isole Salomone, Il livello governativo di Isole Salomone presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Isole Salomone, Sul piano militare e dual-use, Isole Salomone mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Isole Salomone, Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Isole Salomone, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,6/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
2,8	2,7	3,5	3,8	3,0	3,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,5	4,7	6,0	6,6	4,7	5,6

Il GCRI di Isole Salomone è 3,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,6/10), mentre il più basso è Maturità cyber (4,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio-alto	Medio-alto	Medio	Medio

La matrice applica il FOTR di 5,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Isole Salomone, 2 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Cloud e infrastrutture, IP e R&S. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Isole Salomone, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Isole Salomone, Dal punto di vista italiano, Isole Salomone rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Isole Salomone è indicata una cooperazione selettiva, coerente con il FOTR di 5,5/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Cloud e infrastrutture a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

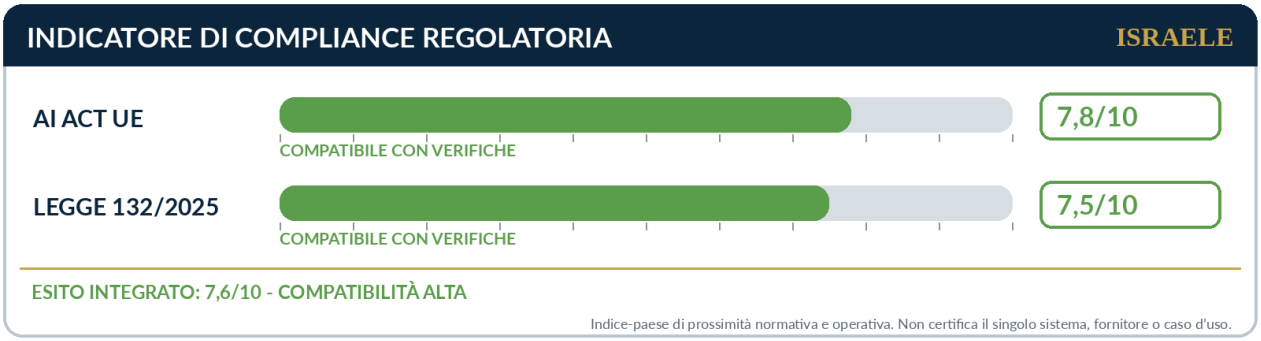
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Isole Salomone: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Israele

Posizione FOTR	44	**Area**	Asia	**Subregione**	Medio Oriente e Asia occidentale
Status	Stato membro delle Nazioni Unite	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	**7,8**	**GCRI / 10**	**7,8**	**Classe operativa**	**Affidabilità favorevole ma condizionata**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Israele, AI Act UE 7,8/10; legge 132/2025 7,5/10; esito integrato 7,6/10, classe «Compatibile con verifiche». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Prima dell'ingaggio occorre una analisi degli scostamenti mirata su trasparenza, governance dei dati, rappresentanza nell'UE, audit e rimedi contrattuali.

Premessa geopolitica e tecnologica

Israele è uno dei principali ecosistemi mondiali per cybersicurezza, difesa, semiconduttori, sorveglianza e intelligenza artificiale. L'elevata capacità tecnica e l'adeguatezza UE per i dati personali favoriscono la cooperazione, mentre il contesto regionale, la forte integrazione tra ricerca civile e difesa e l'intensità delle operazioni di sicurezza richiedono una valutazione rigorosa di utilizzatore finale e destinazione d'uso, accessi privilegiati, esportazioni dual-use e continuità. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 73/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,8/10) e indice FOTR (7,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Elevata capacità cyber, innovazione e cooperazione tecnologica; il contesto di sicurezza e gli accessi pubblici richiedono una valutazione specifica per dati sensibili e dual-use.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	88,2% / 29,2 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 12.319 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	90,1 / 62,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	93,6/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	73,6/100 - rank 16	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (73/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	9,0 / 5,5 / 6,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Israele, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Israele le evidenze principali sono GTMI 62,9/100, EGDI 90,1/100, GCI 93,6/100, AI readiness 73,6/100. La dimensione più robusta è maturità infrastrutturale (8,9/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Israele è 8,9/10. La base statistica rileva utenti Internet pari al 88,2% nel 2024; 29,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 12.319 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Israele al posto 16 con un valore medio di 73,6/100; il pilastro migliore è politiche pubbliche (92,0/100), quello più debole è resilienza (61,3/100). Il GTMI 2025 è 62,9/100. Il punteggio S2 è 7,2/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Israele è valutata sufficiente ma disomogenea, con S3 pari a 7,9/10. Le evidenze disponibili comprendono indice UN di capitale umano 87,4/100, sviluppo e diffusione dell'IA 64,7/100, penetrazione Internet 88,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Israele ottiene S4 6,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Israele, Forte capacità domestica cyber e dual-use, integrata con ecosistema statunitense ed europeo. L'impatto sulla valutazione è misurato da S4=6,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Israele è S5 8,8/10. La base ITU registra ITU GCI 93,6/100, Tier 2 - avanzato; il pilastro relativamente più debole è misure tecniche (17,9/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (73/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Privacy Protection Law, regolamenti sulla sicurezza dei dati e supervisione nazionale; decisione UE di adeguatezza, da integrare con valutazioni settoriali e geopolitiche.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	9,0	Crimini finanziari	7,0
Reti criminali	4,0	Attori incorporati nello Stato	5,5
Attori stranieri	4,0	Attori del settore privato	5,0
Resilienza complessiva	5,5	Cooperazione internazionale	5,5
Politiche e norme nazionali	6,5	Forze dell'ordine	5,5
Antiriciclaggio	7,0	Prevenzione	6,5
Supporto vittime e testimoni	6,0	Rischio operativo FOTR-CY	6,2 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Israele restituisce un rischio FOTR-CY di 6,2/10 (significativo). La componente cyber-dipendente vale 9,0/10 e quella finanziaria 7,0/10; la risposta sistemica è valutata intermedia, con resilienza media di 5,5/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (5,5/10) e attori del settore privato (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Israele assumono particolare rilevanza phishing e credential theft, ransomware, frodi d'investimento, attacchi a energia e servizi pubblici, abuso di cripto-attività e campagne che possono combinare profitto, spionaggio e pressione politica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Israele, la resilienza complessiva è intermedia (5,5/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 7,0/10, prevenzione 6,5/10 e supporto a vittime e testimoni 6,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Israele, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Israele. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Israele, In Israele le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Israele, Il livello governativo di Israele presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Israele, Sul piano militare e dual-use, Israele mostra stretta cooperazione con ecosistemi occidentali e capacità dual-use significative. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Israele, Privacy Protection Law, regolamenti sulla sicurezza dei dati e supervisione nazionale; decisione UE di adeguatezza, da integrare con valutazioni settoriali e geopolitiche. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Israele, È disponibile una decisione UE di adeguatezza. L'operatore italiano deve comunque controllare la portata della decisione, i trasferimenti successivi, le misure di sicurezza e le eventuali discipline settoriali. La componente FOTR di trasferibilità è 10,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,9	7,2	7,9	6,1	8,8	7,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
7,8	8,6	6,2	6,6	7,5	10,0

Il GCRI di Israele è 7,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 7,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (10,0/10), mentre il più basso è Trasparenza istituzionale (6,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio

La matrice applica il FOTR di 7,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Israele, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Israele, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Israele, Dal punto di vista italiano, Israele rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Israele è favorevole ma condizionata: il valore FOTR di 7,8/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Trasparenza istituzionale.

Presidi minimi raccomandati

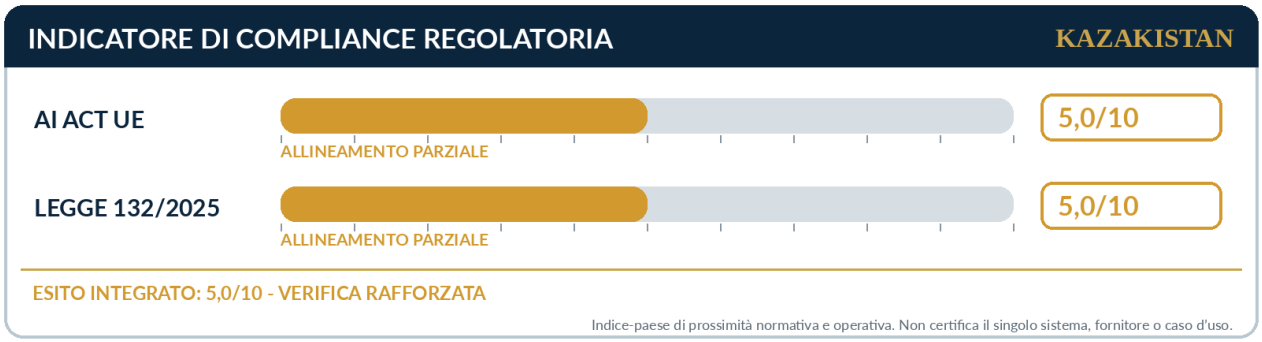
Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Israele: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Kazakistan

Posizione FOTR	137	Area	Asia	Subregione	Caucaso e Asia centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	4,8	GCRI / 10	6,8	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Kazakistan, AI Act UE 5,0/10; legge 132/2025 5,0/10; esito integrato 5,0/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Kazakistan, situato in Caucaso e Asia centrale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, Russia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 23/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (6,8/10) è superiore al punteggio FOTR (4,8/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Kazakistan è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	93,4% / 15,3 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 6.914 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	90,1 / 94,5	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	94,0/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	59,6/100 - rank 58	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	37/100 - Non libero / Non libero (23/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Firmatario/invitato	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,0 / 4,7 / 4,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Kazakistan, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Kazakistan le evidenze principali sono GTMI 94,5/100, EGDI 90,1/100, GCI 94,0/100, AI readiness 59,6/100. La dimensione più robusta è maturità infrastrutturale (8,2/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,5/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Kazakistan è 8,2/10. La base statistica rileva utenti Internet pari al 93,4% nel 2024; 15,3 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 6.914 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Kazakistan al posto 58 con un valore medio di 59,6/100; il pilastro migliore è politiche pubbliche (88,0/100), quello più debole è resilienza (37,4/100). Il GTMI 2025 è 94,5/100. Il punteggio S2 è 7,0/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Kazakistan è valutata sufficiente ma disomogenea, con S3 pari a 6,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 84,0/100, sviluppo e diffusione dell'IA 39,9/100, penetrazione Internet 93,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Kazakistan ottiene S4 5,5/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, Russia; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Kazakistan, Mix russo-cinese, con presenza europea e statunitense nei segmenti commerciali e industriali. L'impatto sulla valutazione è misurato da S4=5,5/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Kazakistan è S5 7,0/10. La base ITU registra ITU GCI 94,0/100, Tier 2 - avanzato; il pilastro relativamente più debole è sviluppo delle capacità (16,4/20). Freedom on the Net è 37/100 - Non libero, mentre Freedom in the World è Non libero (23/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Firmatario/invitato. Quadro normativo sintetico: Legge sui dati personali, localizzazione e controllo delle telecomunicazioni; ecosistema fortemente influenzato da Russia e Cina.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,0	Crimini finanziari	6,0
Reti criminali	5,0	Attori incorporati nello Stato	6,0
Attori stranieri	4,0	Attori del settore privato	4,0
Resilienza complessiva	4,7	Cooperazione internazionale	5,5
Politiche e norme nazionali	5,5	Forze dell'ordine	4,5
Antiriciclaggio	4,5	Prevenzione	4,5
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	4,9 - MODERATO

Pressione del crimine digitale. Il profilo di Kazakistan restituisce un rischio FOTR-CY di 4,9/10 (moderato). La componente cyber-dipendente vale 4,0/10 e quella finanziaria 6,0/10; la risposta sistemica è valutata debole, con resilienza media di 4,7/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (6,0/10) e reti criminali (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Kazakistan assumono particolare rilevanza ransomware come servizio, malware sottrattori di informazioni, infrastrutture di hosting permissive, DDoS, furto di credenziali, estorsione dei dati e possibili sovrapposizioni tra criminalità professionale e finalità geopolitiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Kazakistan, la resilienza complessiva è debole (4,7/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 4,5/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Kazakistan, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; blocco di hosting e ASN ad alta reputazione negativa, ricerca proattiva delle minacce su malware sottrattori di informazioni e controllo dei canali RDP/VPN; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Kazakistan. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Kazakistan, In Kazakistan le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Kazakistan, Il livello governativo di Kazakistan presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Kazakistan, Sul piano militare e dual-use, Kazakistan mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Kazakistan, Legge sui dati personali, localizzazione e controllo delle telecomunicazioni; ecosistema fortemente influenzato da Russia e Cina. Lo stato rispetto alla Convenzione di Budapest è: Firmatario/invitato; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Kazakistan, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 3,7/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,2	7,0	6,5	5,5	7,0	6,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,8	5,5	4,7	5,2	5,1	3,7

Il GCRI di Kazakistan è 6,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (5,5/10), mentre il più basso è Trasferibilità dati (3,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Kazakistan, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Kazakistan, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Kazakistan, Dal punto di vista italiano, Kazakistan rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Kazakistan ricade nella fascia di alto rischio (4,8/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.
Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

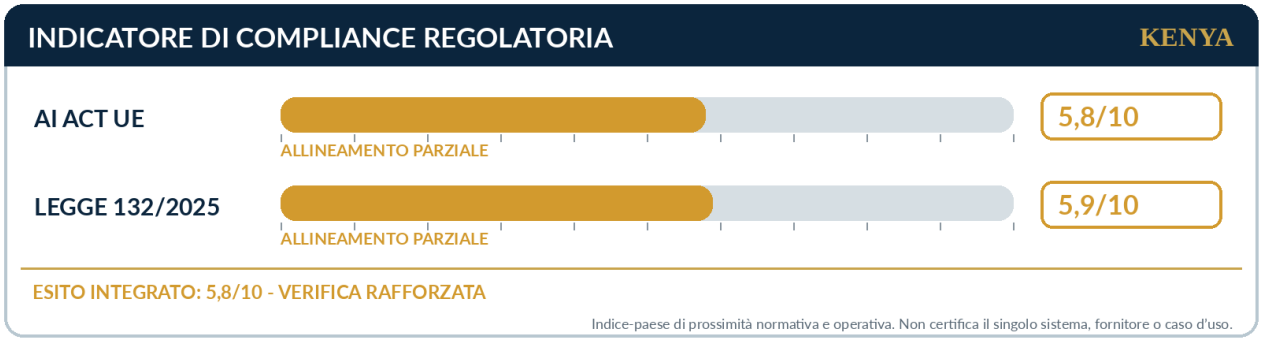
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Kazakistan: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Kenya

Posizione FOTR	87	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,8	GCRI / 10	5,7	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Kenya, AI Act UE 5,8/10; legge 132/2025 5,9/10; esito integrato 5,8/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Kenya non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 49/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,7/10) e indice FOTR (5,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il quadro di Kenya è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	35,0% / 3,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	77,0% / 400 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	63,1 / 77,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	98,6/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	57,9/100 - rank 68	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	58/100 - Parzialmente libero / Parzialmente libero (49/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Firmatario/invitato	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	8,0 / 5,2 / 7,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Kenya, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Kenya le evidenze principali sono GTMI 77,0/100, EGDI 63,1/100, GCI 98,6/100, AI readiness 57,9/100. La dimensione più robusta è postura di sicurezza cyber (7,9/10), mentre la criticità relativa riguarda maturità infrastrutturale (4,5/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Kenya è 4,5/10. La base statistica rileva utenti Internet pari al 35,0% nel 2024; 3,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 77,0% nel 2024; 400 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Kenya al posto 68 con un valore medio di 57,9/100; il pilastro migliore è resilienza (70,7/100), quello più debole è sviluppo e diffusione (35,5/100). Il GTMI 2025 è 77,0/100. Il punteggio S2 è 6,2/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Kenya è valutata sufficiente ma disomogenea, con S3 pari a 5,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 52,7/100, sviluppo e diffusione dell'IA 35,5/100, penetrazione Internet 35,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Kenya ottiene S4 4,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 3,6/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Kenya, Forte presenza cinese nelle reti, affiancata da operatori statunitensi, europei, indiani e locali. L'impatto sulla valutazione è misurato da S4=4,6/10 e dal proxy di indipendenza 3,6/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Kenya è S5 7,9/10. La base ITU registra ITU GCI 98,6/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure tecniche (19,1/20). Freedom on the Net è 58/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (49/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Firmatario/invitato. Quadro normativo sintetico: Data Protection Act 2019, Office of the Data Protection Commissioner e Computer Misuse and Cybercrimes Act; quadro in consolidamento.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	8,0	Crimini finanziari	8,0
Reti criminali	8,0	Attori incorporati nello Stato	8,0
Attori stranieri	6,5	Attori del settore privato	6,0
Resilienza complessiva	5,2	Cooperazione internazionale	7,5
Politiche e norme nazionali	7,0	Forze dell'ordine	5,0
Antiriciclaggio	5,5	Prevenzione	3,5
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	7,1 - ALTO

Quadro criminale digitale. Per Kenya, l'indice operativo FOTR-CY è 7,1/10, classe alta. Il mercato dei reati cyber-dipendenti è molto elevato (8,0/10), mentre i crimini finanziari sono molto elevati (8,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (8,0/10) e attori incorporati nello Stato (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Kenya assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Kenya, la resilienza complessiva è debole (5,2/10); la cooperazione internazionale è robusta (7,5/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 3,5/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Kenya, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Kenya. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Kenya, In Kenya le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Kenya, Il livello governativo di Kenya presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Kenya, Sul piano militare e dual-use, Kenya mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Kenya, Data Protection Act 2019, Office of the Data Protection Commissioner e Computer Misuse and Cybercrimes Act; quadro in consolidamento. Lo stato rispetto alla Convenzione di Budapest è: Firmatario/invitato; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Kenya, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,6/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
4,5	6,2	5,2	4,6	7,9	5,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,6	5,9	5,9	6,3	5,6	5,6

Il GCRI di Kenya è 5,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,3/10), mentre il più basso è Compatibilità giuridica (5,6/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Kenya, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Kenya, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Kenya, Dal punto di vista italiano, Kenya rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Kenya è indicata una cooperazione selettiva, coerente con il FOTR di 5,8/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Compatibilità giuridica a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

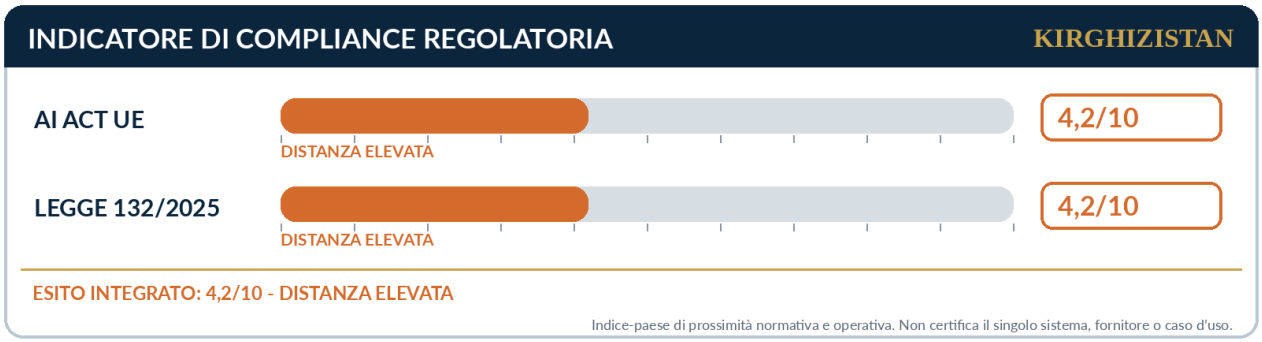
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Kenya: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Kirghizistan

Posizione FOTR	173	Area	Asia	Subregione	Caucaso e Asia centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	4,2	GCRI / 10	5,5	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Kirghizistan, AI Act UE 4,2/10; legge 132/2025 4,2/10; esito integrato 4,2/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Kirghizistan è stato membro delle nazioni unite collocato in Caucaso e Asia centrale. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina, Russia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 25/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (5,5/10) è superiore al punteggio FOTR (4,2/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Kirghizistan presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	92,0% / 7,8 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 1.302 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	73,2 / 62,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	65,6/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	32,5/100 - rank 119	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	47/100 - Parzialmente libero / Non libero (25/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 3,8 / 5,3	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Kirghizistan, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Kirghizistan le evidenze principali sono GTMI 62,6/100, EGDI 73,2/100, GCI 65,6/100, AI readiness 32,5/100. La dimensione più robusta è maturità infrastrutturale (7,5/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,3/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Kirghizistan è 7,5/10. La base statistica rileva utenti Internet pari al 92,0% nel 2024; 7,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 1.302 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Kirghizistan al posto 119 con un valore medio di 32,5/100; il pilastro migliore è adozione pubblica (46,9/100), quello più debole è politiche pubbliche (16,0/100). Il GTMI 2025 è 62,6/100. Il punteggio S2 è 4,3/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Kirghizistan è valutata fragile, con S3 pari a 4,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 70,6/100, sviluppo e diffusione dell'IA 22,1/100, penetrazione Internet 92,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Kirghizistan ottiene S4 5,5/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina, Russia; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Kirghizistan, Forte influenza russa e cinese, con mercato multi-fornitore di piccola scala. L'impatto sulla valutazione è misurato da S4=5,5/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Kirghizistan è S5 5,6/10. La base ITU registra ITU GCI 65,6/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (5,5/20). Freedom on the Net è 47/100 - Parzialmente libero, mentre Freedom in the World è Non libero (25/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Legge sulle informazioni personali e disciplina cyber in evoluzione; capacità istituzionale e continuità da verificare.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	6,5
Reti criminali	5,5	Attori incorporati nello Stato	8,5
Attori stranieri	4,5	Attori del settore privato	4,0
Resilienza complessiva	3,8	Cooperazione internazionale	4,5
Politiche e norme nazionali	4,0	Forze dell'ordine	3,5
Antiriciclaggio	3,5	Prevenzione	5,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	5,3 - SIGNIFICATIVO

Quadro criminale digitale. Per Kirghizistan, l'indice operativo FOTR-CY è 5,3/10, classe significativa. Il mercato dei reati cyber-dipendenti è limitato o poco osservabile (3,0/10), mentre i crimini finanziari sono elevati (6,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,5/10) e reti criminali (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Kirghizistan assumono particolare rilevanza ransomware come servizio, malware sottrattori di informazioni, infrastrutture di hosting permissive, DDoS, furto di credenziali, estorsione dei dati e possibili sovrapposizioni tra criminalità professionale e finalità geopolitiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Kirghizistan, la resilienza complessiva è debole (3,8/10); la cooperazione internazionale è debole (4,5/10), le politiche e norme nazionali sono deboli (4,0/10) e la capacità delle forze dell'ordine è debole (3,5/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 5,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Kirghizistan, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; blocco di hosting e ASN ad alta reputazione negativa, ricerca proattiva delle minacce su malware sottrattori di informazioni e controllo dei canali RDP/VPN; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Kirghizistan. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Kirghizistan, In Kirghizistan le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i

partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Kirghizistan, Il livello governativo di Kirghizistan presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Kirghizistan, Sul piano militare e dual-use, Kirghizistan mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Kirghizistan, Legge sulle informazioni personali e disciplina cyber in evoluzione; capacità istituzionale e continuità da verificare. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Kirghizistan, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,1/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,5	4,3	4,8	5,5	5,6	5,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,1	4,8	3,8	4,1	4,6	4,1

Il GCRI di Kirghizistan è 5,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (4,8/10), mentre il più basso è Trasparenza istituzionale (3,8/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Kirghizistan, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Kirghizistan, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Kirghizistan, Dal punto di vista italiano, Kirghizistan rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Kirghizistan ricade nella fascia di alto rischio (4,2/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

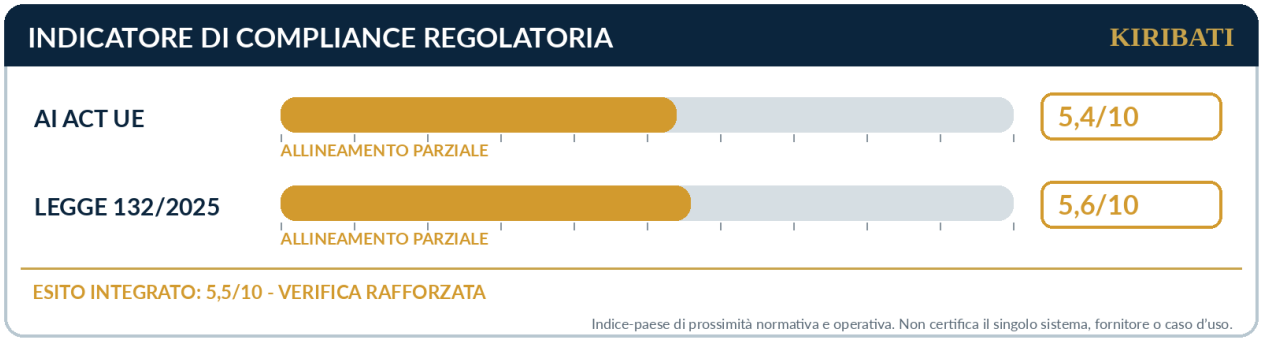
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Kirghizistan: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Kiribati

Posizione FOTR	99	Area	Oceania	Subregione	Pacifico insulare
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,7	GCRI / 10	4,3	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Kiribati, AI Act UE 5,4/10; legge 132/2025 5,6/10; esito integrato 5,5/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Oceania, Kiribati presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La distanza geografica e l'insularità rendono centrali cavi sottomarini, satelliti, continuità energetica e dipendenza da fornitori australiani, neozelandesi, statunitensi o asiatici. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 89/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,7/10) supera il GCRI tecnico (4,3/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. In Kiribati la trasformazione digitale procede più rapidamente dell'uniformità regolatoria e operativa. Gli investimenti devono essere accompagnati da audit, clausole di uscita e gestione locale del rischio.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	89,4% / 0,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	97,7% / 22 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	45,7 / 25,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	55,6/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	22,1/100 - rank 150	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (89/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 4,5 / 3,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Kiribati, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Kiribati le evidenze principali sono GTMI 25,4/100, EGDI 45,7/100, GCI 55,6/100, AI readiness 22,1/100. La dimensione più robusta è postura di sicurezza cyber (5,5/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,7/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Kiribati è 4,9/10. La base statistica rileva utenti Internet pari al 89,4% nel 2024; 0,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 97,7% nel 2024; 22 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Kiribati al posto 150 con un valore medio di 22,1/100; il pilastro migliore è resilienza (41,6/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 25,4/100. Il punteggio S2 è 2,7/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Kiribati è valutata fragile, con S3 pari a 4,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 62,7/100, sviluppo e diffusione dell'IA 19,8/100, penetrazione Internet 89,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Kiribati ottiene S4 4,1/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Kiribati, Dipendenza da Australia, Nuova Zelanda, Stati Uniti, Francia e operatori satellitari o sottomarini; la scala ridotta limita la diversificazione e aumenta il rischio di concentrazione. L'impatto sulla

valutazione è misurato da S4=4,1/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Kiribati è S5 5,5/10. La base ITU registra ITU GCI 55,6/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (2,4/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (89/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	4,0
Reti criminali	4,0	Attori incorporati nello Stato	1,5
Attori stranieri	3,0	Attori del settore privato	2,0
Resilienza complessiva	4,5	Cooperazione internazionale	5,0
Politiche e norme nazionali	6,0	Forze dell'ordine	5,0
Antiriciclaggio	4,0	Prevenzione	3,0
Supporto vittime e testimoni	1,5	Rischio operativo FOTR-CY	3,4 - MODERATO

Rischio criminale connesso alle tecnologie. In Kiribati il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 3,4/10, livello moderato. I reati che dipendono direttamente da sistemi informatici raggiungono 2,0/10; le frodi e i reati finanziari 4,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (4,0/10) e attori stranieri (3,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Kiribati assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Kiribati, la resilienza complessiva è debole (4,5/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 3,0/10 e supporto a vittime e testimoni 1,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Kiribati, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Kiribati. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Kiribati, In Kiribati le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Kiribati, Il livello governativo di Kiribati presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il

settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Kiribati, Sul piano militare e dual-use, Kiribati mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Kiribati, Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Kiribati, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,3/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
4,9	2,7	4,4	4,1	5,5	4,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,0	5,2	6,0	6,7	4,4	5,3

Il GCRI di Kiribati è 4,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,7/10), mentre il più basso è Supply chain (4,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio-alto	Medio	Medio	Medio

La matrice applica il FOTR di 5,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Kiribati, 1 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Cloud e infrastrutture. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Kiribati, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Kiribati, Dal punto di vista italiano, Kiribati rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Kiribati è indicata una cooperazione selettiva, coerente con il FOTR di 5,7/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Cloud e infrastrutture a decisione caso per caso.

Presidi minimi raccomandati

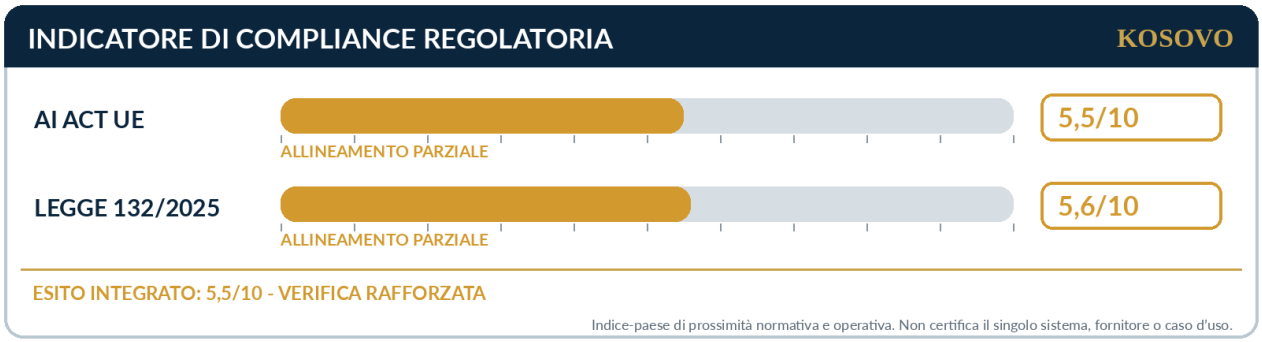
- Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
- Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
- Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
- Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Kiribati: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Kosovo

Posizione FOTR	114	Area	Europa	Subregione	Europa sud-orientale
Status	Entità statuale a riconoscimento parziale	Confidenza Celeborn Intelligence	Bassa	Copertura dati	0/7 famiglie
FOTR / 10	5,5	GCRI / 10	5,2	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Kosovo, AI Act UE 5,5/10; legge 132/2025 5,6/10; esito integrato 5,5/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Kosovo, situato in Europa sud-orientale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La prossimità europea può ridurre i costi operativi, ma non sostituisce la verifica dell'allineamento al GDPR, delle autorità indipendenti e della reale origine dei servizi cloud. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 61/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,2/10) e indice FOTR (5,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Mercato in convergenza europea, con capacità istituzionale in crescita; il riconoscimento non universale e la dipendenza da infrastrutture esterne incidono su contratti e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	n.d. / n.d. per 100	n.d./n.d.	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	n.d. / n.d. per milione	n.d./n.d.	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	n.d. / n.d.	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	n.d./100 - n.d.	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	n.d./100 - rank n.d.	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (61/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,3 / 5,1 / 5,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Kosovo, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 0/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Kosovo le evidenze principali sono nessun indicatore composito pienamente comparabile. La dimensione più robusta è adozione di IA e tecnologie emergenti (5,4/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (5,0/10). Sono disponibili 0 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata bassa. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Kosovo è 5,3/10. La base statistica rileva i principali dati WDI non sono disponibili in forma omogenea. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Per Kosovo non è disponibile un profilo Oxford Insights direttamente attribuibile; l'adozione di IA è quindi valutata attraverso GovTech, servizi online, infrastrutture e fonti qualitative. Il punteggio S2 è 5,4/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Kosovo è valutata sufficiente ma disomogenea, con S3 pari a 5,0/10. Le evidenze disponibili comprendono evidenza quantitativa incompleta. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Kosovo ottiene S4 5,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Kosovo, Fornitori europei e statunitensi, operatori regionali e dipendenza da collegamenti transfrontalieri. L'impatto sulla valutazione è misurato da S4=5,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Kosovo è S5 5,1/10. La base ITU registra GCI non disponibile in forma comparabile. Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (61/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro nazionale di protezione dati e cybersicurezza in progressivo allineamento all'acquis dell'Unione europea; la distanza tra legge formale, vigilanza e prassi deve essere verificata nel settore interessato.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,3	Crimini finanziari	6,4
Reti criminali	6,8	Attori incorporati nello Stato	7,1
Attori stranieri	4,8	Attori del settore privato	5,2
Resilienza complessiva	5,1	Cooperazione internazionale	6,7
Politiche e norme nazionali	5,2	Forze dell'ordine	5,3
Antiriciclaggio	5,2	Prevenzione	5,3
Supporto vittime e testimoni	4,3	Rischio operativo FOTR-CY	5,8 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Kosovo il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,8/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 5,3/10; le frodi e i reati finanziari 6,4/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,1/10) e reti criminali (6,8/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Kosovo assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Kosovo, la resilienza complessiva è debole (5,1/10); la cooperazione internazionale è intermedia (6,7/10), le politiche e norme nazionali sono deboli (5,2/10) e la capacità delle forze dell'ordine è debole (5,3/10). Completano il quadro antiriciclaggio 5,2/10, prevenzione 5,3/10 e supporto a vittime e testimoni 4,3/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Kosovo, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative. Poiché l'entità non dispone di una serie nazionale GI-TOC autonoma, i valori derivano da un proxy Celeborn Intelligence ponderato su Albania 40%, Serbia 40%, Macedonia del Nord 20%; la confidenza deve pertanto essere considerata inferiore e la decisione resa più prudente.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; proxy Celeborn Intelligence ponderato su Albania 40%, Serbia 40%, Macedonia del Nord 20%. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Kosovo, In Kosovo le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Kosovo, Il livello governativo di Kosovo presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Kosovo, Sul piano militare e dual-use, Kosovo mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Kosovo, Quadro nazionale di protezione dati e cybersicurezza in progressivo allineamento all'acquis dell'Unione europea; la distanza tra legge formale, vigilanza e prassi deve essere verificata nel settore interessato. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Kosovo, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,2/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
5,3	5,4	5,0	5,1	5,1	5,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,9	5,2	5,0	6,3	5,2	5,2

Il GCRI di Kosovo è 5,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,3/10), mentre il più basso è Trasparenza istituzionale (5,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio

La matrice applica il FOTR di 5,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Kosovo, 4 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Kosovo, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Kosovo, Dal punto di vista italiano, Kosovo rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Kosovo è indicata una cooperazione selettiva, coerente con il FOTR di 5,5/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Sanità e biometria a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

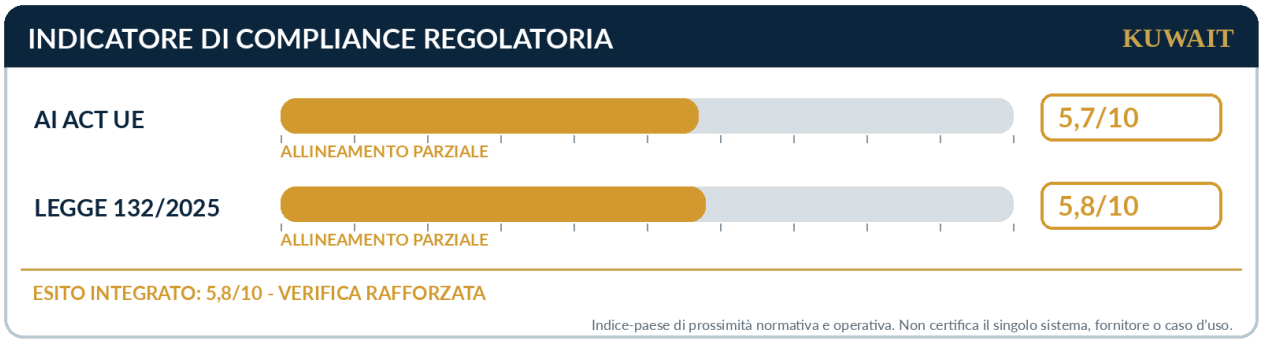
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Kosovo: World Development Indicators, valori più recenti disponibili 2022-2024; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Bassa con copertura 0/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Kuwait

Posizione FOTR	**88**	**Area**	Asia	**Subregione**	Medio Oriente e Asia occidentale
Status	**Stato membro delle Nazioni Unite**	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	**5,8**	**GCRI / 10**	**6,0**	**Classe operativa**	**Affidabilità selettiva**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Kuwait, AI Act UE 5,7/10; legge 132/2025 5,8/10; esito integrato 5,8/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Kuwait non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 30/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,0/10) e indice FOTR (5,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Kuwait dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	100,0% / 1,0 per 100	2025/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 384 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	78,1 / 68,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	60,6/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	43,4/100 - rank 83	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (30/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,0 / 5,4 / 5,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Kuwait, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Kuwait le evidenze principali sono GTMI 68,4/100, EGDI 78,1/100, GCI 60,6/100, AI readiness 43,4/100. La dimensione più robusta è maturità infrastrutturale (7,7/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (5,2/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Kuwait è 7,7/10. La base statistica rileva utenti Internet pari al 100,0% nel 2025; 1,0 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 100,0% nel 2024; 384 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Kuwait al posto 83 con un valore medio di 43,4/100; il pilastro migliore è infrastrutture IA (53,3/100), quello più debole è sviluppo e diffusione (30,2/100). Il GTMI 2025 è 68,4/100. Il punteggio S2 è 5,2/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Kuwait è valutata sufficiente ma disomogenea, con S3 pari a 5,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 70,8/100, sviluppo e diffusione dell'IA 30,2/100, penetrazione Internet 100,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Kuwait ottiene S4 5,6/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Kuwait, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo societario e

subfornitura. L'impatto sulla valutazione è misurato da S4=5,6/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Kuwait è S5 6,0/10. La base ITU registra ITU GCI 60,6/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (5,8/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (30/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa settoriale su telecomunicazioni, cloud e protezione dei dati, senza un regime unitario pienamente assimilabile al GDPR; necessarie clausole e segregazione tecnica.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,0	Crimini finanziari	7,0
Reti criminali	6,0	Attori incorporati nello Stato	6,0
Attori stranieri	3,5	Attori del settore privato	6,5
Resilienza complessiva	5,4	Cooperazione internazionale	6,0
Politiche e norme nazionali	5,5	Forze dell'ordine	6,0
Antiriciclaggio	5,5	Prevenzione	5,5
Supporto vittime e testimoni	5,5	Rischio operativo FOTR-CY	5,8 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (7,0/10), criminalità finanziaria (7,0/10) e resilienza (5,4/10) colloca Kuwait in una fascia di rischio significativo, pari a 5,8/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori del settore privato (6,5/10) e reti criminali (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Kuwait assumono particolare rilevanza phishing e credential theft, ransomware, frodi d'investimento, attacchi a energia e servizi pubblici, abuso di cripto-attività e campagne che possono combinare profitto, spionaggio e pressione politica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Kuwait, la resilienza complessiva è debole (5,4/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è intermedia (6,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 5,5/10 e supporto a vittime e testimoni 5,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Kuwait, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Kuwait. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Kuwait, In Kuwait le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Kuwait, Il livello governativo di Kuwait presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Kuwait, Sul piano militare e dual-use, Kuwait mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Kuwait, Normativa settoriale su telecomunicazioni, cloud e protezione dei dati, senza un regime unitario pienamente assimilabile al GDPR; necessarie clausole e segregazione tecnica. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Kuwait, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,4/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,7	5,2	5,6	5,6	6,0	6,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,8	6,2	5,6	5,8	6,1	5,4

Il GCRI di Kuwait è 6,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Maturità cyber (6,2/10), mentre il più basso è Trasferibilità dati (5,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Kuwait, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Kuwait, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Kuwait, Dal punto di vista italiano, Kuwait rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Kuwait è indicata una cooperazione selettiva, coerente con il FOTR di 5,8/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasferibilità dati a decisione caso per caso.

Presidi minimi raccomandati

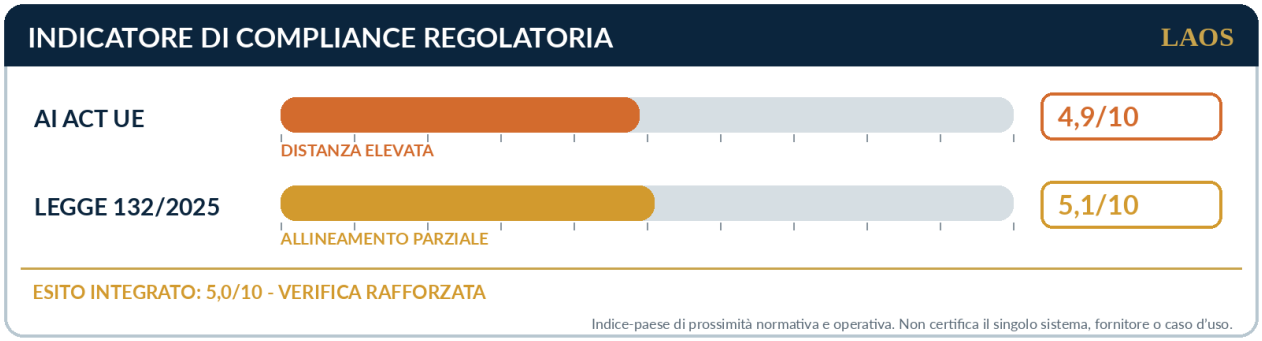
Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Kuwait: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Laos

Posizione FOTR	132	Area	Asia	Subregione	Asia sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,1	GCRI / 10	4,3	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Laos, AI Act UE 4,9/10; legge 132/2025 5,1/10; esito integrato 5,0/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Laos è stato membro delle nazioni unite collocato in Asia sud-orientale. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 13/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (4,3/10) e indice FOTR (5,1/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per Laos non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	65,6% / 2,7 per 100	2024/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	96,5% / 302 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	44,0 / 40,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	33,7/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	29,8/100 - rank 125	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (13/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 3,4 / 6,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Laos, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Laos le evidenze principali sono GTMI 40,4/100, EGDI 44,0/100, GCI 33,7/100, AI readiness 29,8/100. La dimensione più robusta è maturità infrastrutturale (5,3/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,3/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Laos è 5,3/10. La base statistica rileva utenti Internet pari al 65,6% nel 2024; 2,7 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 96,5% nel 2024; 302 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Laos al posto 125 con un valore medio di 29,8/100; il pilastro migliore è governance (45,2/100), quello più debole è adozione pubblica (18,2/100). Il GTMI 2025 è 40,4/100. Il punteggio S2 è 3,3/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Laos è valutata fragile, con S3 pari a 4,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 46,1/100, sviluppo e diffusione dell'IA 20,9/100, penetrazione Internet 65,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Laos ottiene S4 4,9/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Laos, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo societario e

subfornitura. L'impatto sulla valutazione è misurato da S4=4,9/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Laos è S5 4,1/10. La base ITU registra ITU GCI 33,7/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è sviluppo delle capacità (2,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (13/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	8,0
Reti criminali	7,0	Attori incorporati nello Stato	7,5
Attori stranieri	8,0	Attori del settore privato	7,0
Resilienza complessiva	3,4	Cooperazione internazionale	4,0
Politiche e norme nazionali	4,0	Forze dell'ordine	4,0
Antiriciclaggio	3,0	Prevenzione	3,5
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	6,8 - ALTO

Pressione del crimine digitale. Il profilo di Laos restituisce un rischio FOTR-CY di 6,8/10 (alto). La componente cyber-dipendente vale 5,5/10 e quella finanziaria 8,0/10; la risposta sistemica è valutata molto debole, con resilienza media di 3,4/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (8,0/10) e attori incorporati nello Stato (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Laos assumono particolare rilevanza centri organizzati di truffa, frodi d'investimento e sentimentali, phishing multicanale, batterie di schede SIM, conti prestanome, riciclaggio in cripto-attività e compromissione di servizi esternalizzati. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Laos, la resilienza complessiva è molto debole (3,4/10); la cooperazione internazionale è debole (4,0/10), le politiche e norme nazionali sono deboli (4,0/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 3,0/10, prevenzione 3,5/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Laos, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; controllo della filiera contro esposizione a complessi organizzati per truffe telematiche, call center coercitivi e conti prestanome; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Laos. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Laos, In Laos le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Laos, Il livello governativo di Laos presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Laos, Sul piano militare e dual-use, Laos mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Laos, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Laos, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,7/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
5,3	3,3	4,0	4,9	4,1	4,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,2	5,6	4,7	5,3	5,3	4,7

Il GCRI di Laos è 4,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,1/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Maturità cyber (5,6/10), mentre il più basso è Trasparenza istituzionale (4,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 5,1/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Laos, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Laos, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Laos, Dal punto di vista italiano, Laos rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Laos è indicata una cooperazione selettiva, coerente con il FOTR di 5,1/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

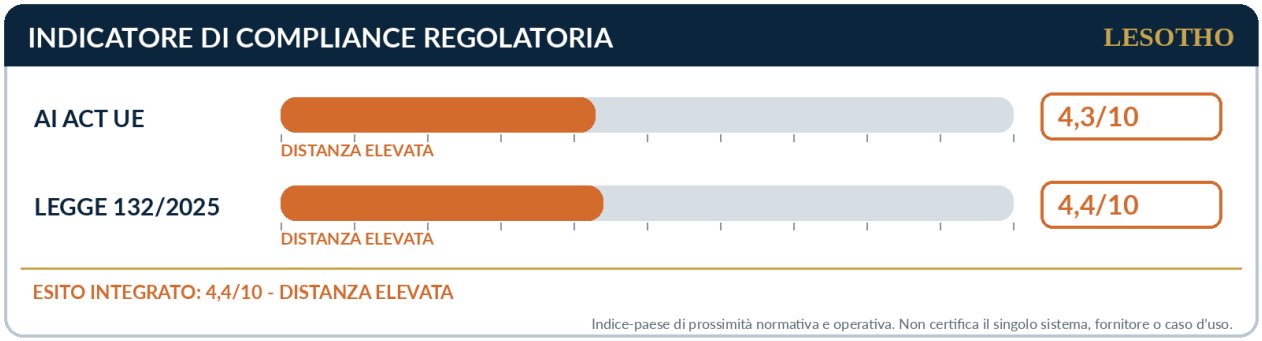
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Laos: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Lesotho

Posizione FOTR	148	Area	Africa	Subregione	Africa australe
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,5	GCRI / 10	3,8	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Lesotho, AI Act UE 4,3/10; legge 132/2025 4,4/10; esito integrato 4,4/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Lesotho presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 67/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (3,8/10) e indice FOTR (4,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per Lesotho non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	51,8% / 0,4 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	60,6% / 86 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	41,2 / 34,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	30,6/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	30,4/100 - rank 131	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (67/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 3,9 / 4,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Lesotho, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Lesotho le evidenze principali sono GTMI 34,3/100, EGDI 41,2/100, GCI 30,6/100, AI readiness 30,4/100. La dimensione più robusta è indipendenza della supply chain (4,6/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Lesotho è 4,0/10. La base statistica rileva utenti Internet pari al 51,8% nel 2024; 0,4 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 60,6% nel 2024; 86 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Lesotho al posto 131 con un valore medio di 30,4/100; il pilastro migliore è governance (38,8/100), quello più debole è sviluppo e diffusione (17,6/100). Il GTMI 2025 è 34,3/100. Il punteggio S2 è 3,1/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Lesotho è valutata fragile, con S3 pari a 3,9/10. Le evidenze disponibili comprendono indice UN di capitale umano 48,6/100, sviluppo e diffusione dell'IA 17,6/100, penetrazione Internet 51,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Lesotho ottiene S4 4,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Lesotho, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,6/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Lesotho è S5 3,6/10. La base ITU registra ITU GCI 30,6/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (2,8/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (67/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	5,0
Reti criminali	5,5	Attori incorporati nello Stato	7,0
Attori stranieri	5,5	Attori del settore privato	2,5
Resilienza complessiva	3,9	Cooperazione internazionale	7,0
Politiche e norme nazionali	4,5	Forze dell'ordine	3,0
Antiriciclaggio	4,0	Prevenzione	3,5
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	4,7 - MODERATO

Rischio criminale connesso alle tecnologie. In Lesotho il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 4,7/10, livello moderato. I reati che dipendono direttamente da sistemi informatici raggiungono 2,0/10; le frodi e i reati finanziari 5,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,0/10) e reti criminali (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Lesotho assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Lesotho, la resilienza complessiva è debole (3,9/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono deboli (4,5/10) e la capacità delle forze dell'ordine è molto debole (3,0/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 3,5/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Lesotho, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Lesotho. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Lesotho, In Lesotho le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Lesotho, Il livello governativo di Lesotho presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Lesotho, Sul piano militare e dual-use, Lesotho mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Lesotho, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Lesotho, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,5/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
4,0	3,1	3,9	4,6	3,6	3,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,4	4,5	4,3	4,8	4,4	4,5

Il GCRI di Lesotho è 3,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (4,8/10), mentre il più basso è Trasparenza istituzionale (4,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Lesotho, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Lesotho, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Lesotho, Dal punto di vista italiano, Lesotho rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Lesotho ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.
Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

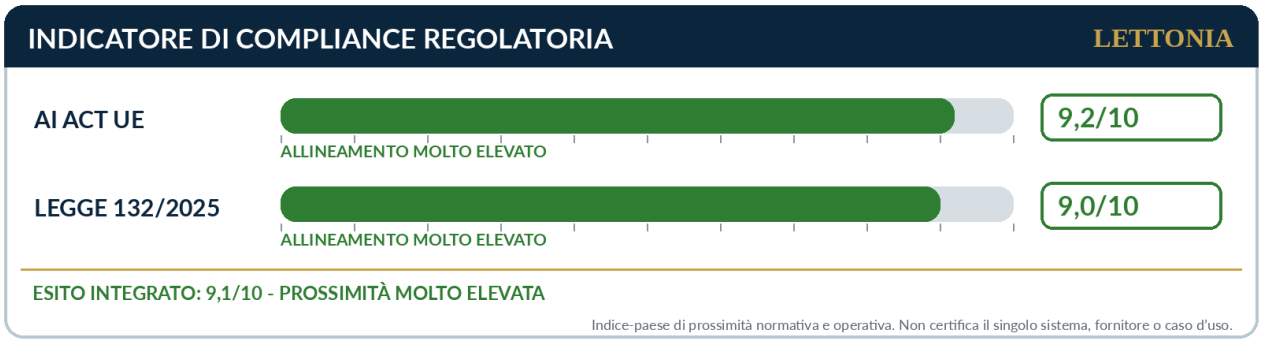
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Lesotho: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Lettonia

Posizione FOTR	28	Area	Europa	Subregione	Europa settentrionale e baltica
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,4	GCRI / 10	7,5	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Lettonia, AI Act UE 9,2/10; legge 132/2025 9,0/10; esito integrato 9,1/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Lettonia, situato in Europa settentrionale e baltica, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 89/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,5/10) e indice FOTR (8,4/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Lettonia combina buona maturità tecnologica e relativa prevedibilità normativa. Il livello di rischio aumenta nei progetti che coinvolgono dati sanitari, identità, infrastrutture critiche o ricerca strategica.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	92,7% / 25,8 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 28.218 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	88,5 / 89,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	82,6/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	62,4/100 - rank 51	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (89/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,0 / 7,6 / 4,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Lettonia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Lettonia le evidenze principali sono GTMI 89,8/100, EGDI 88,5/100, GCI 82,6/100, AI readiness 62,4/100. La dimensione più robusta è maturità infrastrutturale (8,9/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,0/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Lettonia è 8,9/10. La base statistica rileva utenti Internet pari al 92,7% nel 2024; 25,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 28.218 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Lettonia al posto 51 con un valore medio di 62,4/100; il pilastro migliore è governance (82,3/100), quello più debole è sviluppo e diffusione (37,2/100). Il GTMI 2025 è 89,8/100. Il punteggio S2 è 6,9/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Lettonia è valutata sufficiente ma disomogenea, con S3 pari a 7,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 88,0/100, sviluppo e diffusione dell'IA 37,2/100, penetrazione Internet 92,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Lettonia ottiene S4 6,0/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Lettonia, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,0/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Lettonia è S5 8,1/10. La base ITU registra ITU GCI 82,6/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (14,1/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (89/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, Personal Data Processing Law e quadro nazionale cyber allineato a NIS2.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,0	Crimini finanziari	6,5
Reti criminali	4,0	Attori incorporati nello Stato	2,5
Attori stranieri	5,0	Attori del settore privato	3,0
Resilienza complessiva	7,6	Cooperazione internazionale	8,5
Politiche e norme nazionali	8,5	Forze dell'ordine	7,5
Antiriciclaggio	6,0	Prevenzione	7,5
Supporto vittime e testimoni	7,5	Rischio operativo FOTR-CY	4,5 - MODERATO

Quadro criminale digitale. Per Lettonia, l'indice operativo FOTR-CY è 4,5/10, classe moderata. Il mercato dei reati cyber-dipendenti è elevato (6,0/10), mentre i crimini finanziari sono elevati (6,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (5,0/10) e reti criminali (4,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Lettonia assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Lettonia, la resilienza complessiva è robusta (7,6/10); la cooperazione internazionale è robusta (8,5/10), le politiche e norme nazionali sono robuste (8,5/10) e la capacità delle forze dell'ordine è robusta (7,5/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 7,5/10 e supporto a vittime e testimoni 7,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Lettonia, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Lettonia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Lettonia, In Lettonia le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Lettonia, Il livello governativo di Lettonia presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Lettonia, Sul piano militare e dual-use, Lettonia mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Lettonia, GDPR, Personal Data Processing Law e quadro nazionale cyber allineato a NIS2. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Lettonia, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,3/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,9	6,9	7,4	6,0	8,1	7,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,0	7,7	8,0	8,9	7,2	9,3

Il GCRI di Lettonia è 7,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,3/10), mentre il più basso è Supply chain (7,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Lettonia, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Lettonia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Lettonia, Dal punto di vista italiano, Lettonia rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Lettonia, il FOTR di 8,4/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (7,2/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

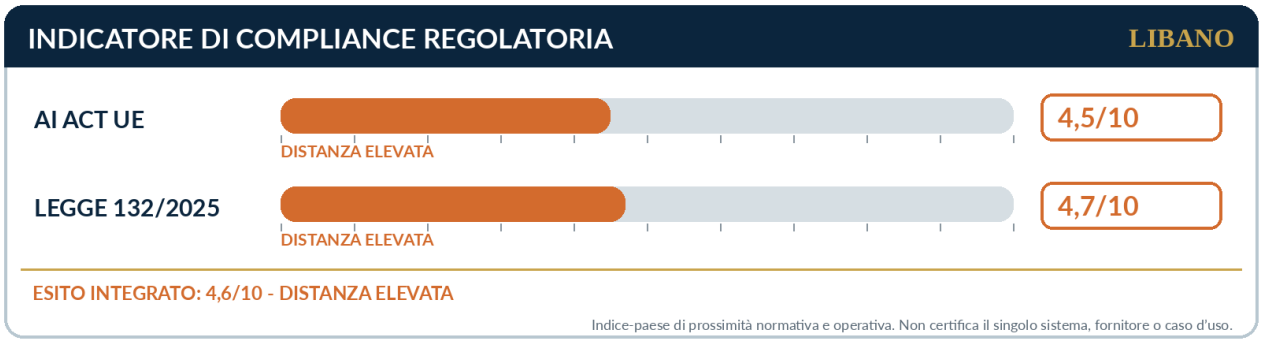
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Lettonia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Libano

Posizione FOTR	142	Area	Asia	Subregione	Medio Oriente e Asia occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	4,6	GCRI / 10	4,5	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Libano, AI Act UE 4,5/10; legge 132/2025 4,7/10; esito integrato 4,6/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Per un operatore italiano, Libano non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 41/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (4,5/10) e indice FOTR (4,6/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Libano è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	80,6% / 7,3 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 267 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	54,5 / 26,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	32,4/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	33,5/100 - rank 117	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	50/100 - Parzialmente libero / Parzialmente libero (41/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 3,1 / 7,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Libano, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Libano le evidenze principali sono GTMI 26,0/100, EGDI 54,5/100, GCI 32,4/100, AI readiness 33,5/100. La dimensione più robusta è maturità infrastrutturale (6,2/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,4/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Libano è 6,2/10. La base statistica rileva utenti Internet pari al 80,6% nel 2024; 7,3 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 100,0% nel 2024; 267 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Libano al posto 117 con un valore medio di 33,5/100; il pilastro migliore è politiche pubbliche (42,0/100), quello più debole è adozione pubblica (18,6/100). Il GTMI 2025 è 26,0/100. Il punteggio S2 è 3,4/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Libano è valutata fragile, con S3 pari a 4,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 54,3/100, sviluppo e diffusione dell'IA 34,1/100, penetrazione Internet 80,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Libano ottiene S4 4,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Libano, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo societario e

subfornitura. L'impatto sulla valutazione è misurato da S4=4,6/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Libano è S5 4,0/10. La base ITU registra ITU GCI 32,4/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (1,4/20). Freedom on the Net è 50/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (41/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	9,0
Reti criminali	7,5	Attori incorporati nello Stato	9,5
Attori stranieri	8,5	Attori del settore privato	8,0
Resilienza complessiva	3,1	Cooperazione internazionale	5,5
Politiche e norme nazionali	3,5	Forze dell'ordine	2,5
Antiriciclaggio	2,5	Prevenzione	3,5
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	7,0 - ALTO

Pressione del crimine digitale. Il profilo di Libano restituisce un rischio FOTR-CY di 7,0/10 (alto). La componente cyber-dipendente vale 4,5/10 e quella finanziaria 9,0/10; la risposta sistemica è valutata molto debole, con resilienza media di 3,1/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,5/10) e attori stranieri (8,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Libano assumono particolare rilevanza phishing e credential theft, ransomware, frodi d'investimento, attacchi a energia e servizi pubblici, abuso di cripto-attività e campagne che possono combinare profitto, spionaggio e pressione politica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Libano, la resilienza complessiva è molto debole (3,1/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono deboli (3,5/10) e la capacità delle forze dell'ordine è molto debole (2,5/10). Completano il quadro antiriciclaggio 2,5/10, prevenzione 3,5/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Libano, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Libano. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Libano, In Libano le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Libano, Il livello governativo di Libano presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Libano, Sul piano militare e dual-use, Libano mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Libano, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Libano, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 3,7/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,2	3,4	4,5	4,6	4,0	4,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,4	4,7	4,1	5,2	4,5	3,7

Il GCRI di Libano è 4,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (5,4/10), mentre il più basso è Trasferibilità dati (3,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Libano, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Libano, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Libano, Dal punto di vista italiano, Libano rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Libano ricade nella fascia di alto rischio (4,6/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

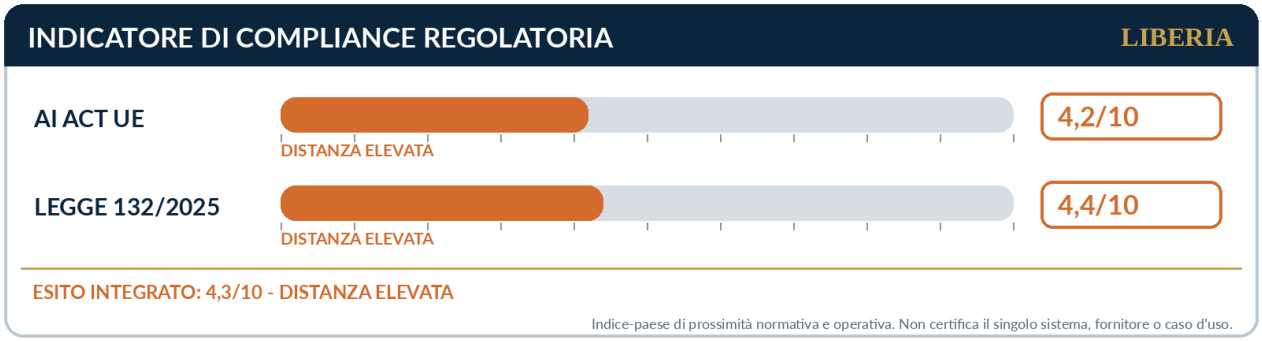
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Libano: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Liberia

Posizione FOTR	166	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,4	GCRI / 10	2,8	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Liberia, AI Act UE 4,2/10; legge 132/2025 4,4/10; esito integrato 4,3/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Liberia è stato membro delle nazioni unite collocato in Africa occidentale. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 65/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (4,4/10) supera il GCRI tecnico (2,8/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Liberia è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	32,2% / 0,3 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	34,9% / 13 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	25,1 / 36,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	21,3/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	14,5/100 - rank 189	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (65/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,0 / 3,4 / 6,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Liberia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Liberia le evidenze principali sono GTMI 36,0/100, EGDI 25,1/100, GCI 21,3/100, AI readiness 14,5/100. La dimensione più robusta è indipendenza della supply chain (4,5/10), mentre la criticità relativa riguarda maturità infrastrutturale (1,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Liberia è 1,9/10. La base statistica rileva utenti Internet pari al 32,2% nel 2024; 0,3 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 34,9% nel 2024; 13 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Liberia al posto 189 con un valore medio di 14,5/100; il pilastro migliore è infrastrutture IA (27,1/100), quello più debole è governance (3,5/100). Il GTMI 2025 è 36,0/100. Il punteggio S2 è 2,1/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Liberia è valutata fragile, con S3 pari a 2,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 36,7/100, sviluppo e diffusione dell'IA 9,8/100, penetrazione Internet 32,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Liberia ottiene S4 4,5/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Liberia, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,5/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Liberia è S5 2,9/10. La base ITU registra ITU GCI 21,3/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (65/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,0	Crimini finanziari	7,5
Reti criminali	7,0	Attori incorporati nello Stato	7,5
Attori stranieri	6,5	Attori del settore privato	6,0
Resilienza complessiva	3,4	Cooperazione internazionale	4,0
Politiche e norme nazionali	4,0	Forze dell'ordine	4,0
Antiriciclaggio	3,5	Prevenzione	2,0
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	6,1 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Liberia presenta un'esposizione stimata significativa (6,1/10): reati cyber-dipendenti 4,0/10, crimini finanziari 7,5/10 e resilienza 3,4/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,5/10) e reti criminali (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Liberia assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Liberia, la resilienza complessiva è molto debole (3,4/10); la cooperazione internazionale è debole (4,0/10), le politiche e norme nazionali sono deboli (4,0/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 2,0/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Liberia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Liberia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Liberia, In Liberia le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner

italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Liberia, Il livello governativo di Liberia presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Liberia, Sul piano militare e dual-use, Liberia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Liberia, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Liberia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,1/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
1,9	2,1	2,6	4,5	2,9	2,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,4	4,2	4,5	5,2	4,3	4,1

Il GCRI di Liberia è 2,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,2/10), mentre il più basso è Trasferibilità dati (4,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Liberia, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Liberia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Liberia, Dal punto di vista italiano, Liberia rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Liberia ricade nella fascia di alto rischio (4,4/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

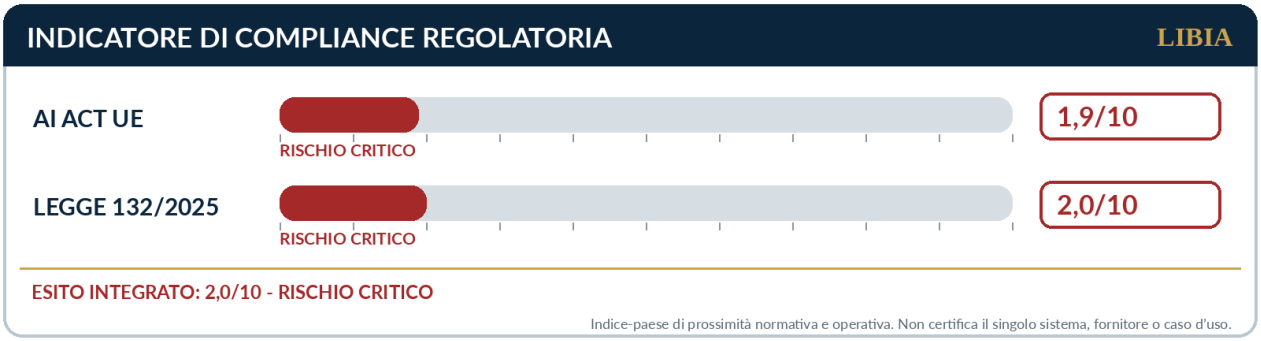
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Liberia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Libia

Posizione FOTR	192	Area	Africa	Subregione	Africa settentrionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	1,8	GCRI / 10	4,0	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Libia, AI Act UE 1,9/10; legge 132/2025 2,0/10; esito integrato 2,0/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Libia presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 10/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (4,0/10) è superiore al punteggio FOTR (1,8/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Libia ricade nella fascia di rischio estremo. L'assenza di rimedi affidabili, le restrizioni, l'instabilità o le sanzioni rendono normalmente incompatibile il trattamento locale di dati italiani sensibili o strategici.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	82,0% / 4,5 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	77,4% / 389 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	54,7 / 20,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	68,1/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	29,4/100 - rank 134	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	43/100 - Parzialmente libero / Non libero (10/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,5 / 1,9 / 6,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Libia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Libia le evidenze principali sono GTMI 20,4/100, EGDI 54,7/100, GCI 68,1/100, AI readiness 29,4/100. La dimensione più robusta è maturità infrastrutturale (6,5/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,6/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Libia è 6,5/10. La base statistica rileva utenti Internet pari al 82,0% nel 2024; 4,5 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 77,4% nel 2024; 389 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Libia al posto 134 con un valore medio di 29,4/100; il pilastro migliore è resilienza (47,6/100), quello più debole è adozione pubblica (2,1/100). Il GTMI 2025 è 20,4/100. Il punteggio S2 è 2,6/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Libia è valutata fragile, con S3 pari a 3,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 59,5/100, sviluppo e diffusione dell'IA 18,9/100, penetrazione Internet 82,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Libia ottiene S4 3,2/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Libia, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=3,2/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Libia è S5 4,0/10. La base ITU registra ITU GCI 68,1/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è cooperazione (10,4/20). Freedom on the Net è 43/100 - Parzialmente libero, mentre Freedom in the World è Non libero (10/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa frammentata e pluralità di centri di potere; accessi pubblici, sicurezza fisica e continuità operativa rendono i progetti digitali ad alto rischio.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,5	Crimini finanziari	9,0
Reti criminali	8,0	Attori incorporati nello Stato	9,5
Attori stranieri	5,5	Attori del settore privato	5,0
Resilienza complessiva	1,9	Cooperazione internazionale	2,5
Politiche e norme nazionali	2,0	Forze dell'ordine	2,0
Antiriciclaggio	2,0	Prevenzione	1,5
Supporto vittime e testimoni	1,0	Rischio operativo FOTR-CY	6,9 - ALTO

Pressione del crimine digitale. Il profilo di Libia restituisce un rischio FOTR-CY di 6,9/10 (alto). La componente cyber-dipendente vale 3,5/10 e quella finanziaria 9,0/10; la risposta sistemica è valutata molto debole, con resilienza media di 1,9/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,5/10) e reti criminali (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Libia assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Libia, la resilienza complessiva è molto debole (1,9/10); la cooperazione internazionale è molto debole (2,5/10), le politiche e norme nazionali sono molto deboli (2,0/10) e la capacità delle forze dell'ordine è molto debole (2,0/10). Completano il quadro antiriciclaggio 2,0/10, prevenzione 1,5/10 e supporto a vittime e testimoni 1,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Libia, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Libia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Libia, In Libia le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. La

disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Libia, Il livello governativo di Libia presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Libia, Sul piano militare e dual-use, Libia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Libia, Normativa frammentata e pluralità di centri di potere; accessi pubblici, sicurezza fisica e continuità operativa rendono i progetti digitali ad alto rischio. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Libia, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 1,4/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,5	2,6	3,8	3,2	4,0	4,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
2,3	1,4	1,7	3,0	1,0	1,4

Il GCRI di Libia è 4,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 1,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (3,0/10), mentre il più basso è Supply chain (1,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 1,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Libia, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Libia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Libia, Dal punto di vista italiano, Libia rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Libia, il FOTR di 1,8/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

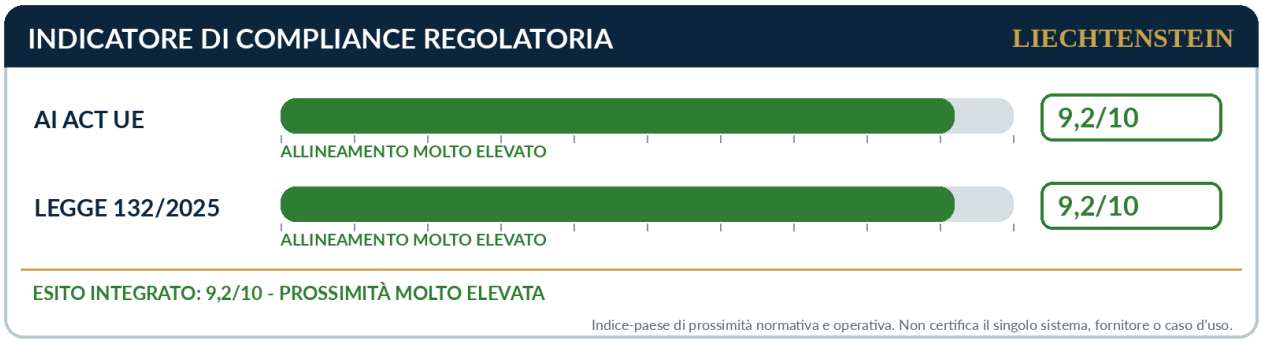
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Libia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Liechtenstein

Posizione FOTR	12	Area	Europa	Subregione	Europa occidentale e centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	9,0	GCRI / 10	6,7	Classe operativa	Affidabilità molto alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Liechtenstein, AI Act UE 9,2/10; legge 132/2025 9,2/10; esito integrato 9,2/10, classe «Allineamento molto elevato». L'integrazione nello Spazio economico europeo riduce la distanza regolatoria, senza eliminare la necessità di verificare autorità competenti, norme settoriali, trasferimenti e catena dei responsabili. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Liechtenstein, situato in Europa occidentale e centrale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La partecipazione allo Spazio economico europeo produce una forte prossimità normativa con l'Italia, pur richiedendo verifiche settoriali e contrattuali. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 90/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (9,0/10) supera il GCRI tecnico (6,7/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il sistema digitale di Liechtenstein è avanzato e integrato con standard internazionali. Le principali criticità non sono di base istituzionale, ma riguardano supply chain, concentrazione dei servizi e gestione delle eccezioni di sicurezza nazionale.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	98,3% / 50,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 60.321 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	85,3 / 55,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	52,0/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	39,9/100 - rank 98	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (90/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,0 / 8,4 / 3,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Liechtenstein, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Liechtenstein le evidenze principali sono GTMI 55,4/100, EGDI 85,3/100, GCI 52,0/100, AI readiness 39,9/100. La dimensione più robusta è maturità infrastrutturale (9,9/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,8/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Liechtenstein è 9,9/10. La base statistica rileva utenti Internet pari al 98,3% nel 2024; 50,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 60.321 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Liechtenstein al posto 98 con un valore medio di 39,9/100; il pilastro migliore è adozione pubblica (49,5/100), quello più debole è politiche pubbliche (19,0/100). Il GTMI 2025 è 55,4/100. Il punteggio S2 è 4,8/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Liechtenstein è valutata sufficiente ma disomogenea, con S3 pari a 6,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 82,6/100, sviluppo e diffusione dell'IA 28,7/100, penetrazione Internet 98,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Liechtenstein ottiene S4 6,0/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open

source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Liechtenstein, Fornitura prevalentemente nazionale, europea e statunitense, con catene hardware globali. In genere è possibile diversificare e imporre requisiti contrattuali elevati. L'impatto sulla valutazione è misurato da S4=6,0/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Liechtenstein è S5 6,4/10. La base ITU registra ITU GCI 52,0/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è organizzazione (3,6/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (90/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR attraverso lo SEE, legge nazionale sulla protezione dei dati e cooperazione EFTA/UE.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,0	Crimini finanziari	7,0
Reti criminali	1,0	Attori incorporati nello Stato	1,0
Attori stranieri	3,0	Attori del settore privato	4,0
Resilienza complessiva	8,4	Cooperazione internazionale	8,0
Politiche e norme nazionali	8,5	Forze dell'ordine	8,5
Antiriciclaggio	5,5	Prevenzione	8,5
Supporto vittime e testimoni	9,5	Rischio operativo FOTR-CY	3,1 - MODERATO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (4,0/10), criminalità finanziaria (7,0/10) e resilienza (8,4/10) colloca Liechtenstein in una fascia di rischio moderato, pari a 3,1/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori del settore privato (4,0/10) e attori stranieri (3,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Liechtenstein assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Liechtenstein, la resilienza complessiva è robusta (8,4/10); la cooperazione internazionale è robusta (8,0/10), le politiche e norme nazionali sono robuste (8,5/10) e la capacità delle forze dell'ordine è robusta (8,5/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 8,5/10 e supporto a vittime e testimoni 9,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Liechtenstein, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Liechtenstein. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Liechtenstein, In Liechtenstein le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione.

Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Liechtenstein, Il livello governativo di Liechtenstein presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Liechtenstein, Sul piano militare e dual-use, Liechtenstein mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Liechtenstein, GDPR attraverso lo SEE, legge nazionale sulla protezione dei dati e cooperazione EFTA/UE. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Liechtenstein, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,8/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,9	4,8	6,5	6,0	6,4	6,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,3	8,6	8,8	9,0	8,8	9,8

Il GCRI di Liechtenstein è 6,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 9,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,8/10), mentre il più basso è Maturità cyber (8,6/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Basso	Basso	Basso

La matrice applica il FOTR di 9,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Liechtenstein, la matrice non individua ambiti ad alto rischio; 6 categorie risultano basse o medio-basse, ferma la verifica del singolo progetto. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Liechtenstein, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Liechtenstein, Dal punto di vista italiano, Liechtenstein rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Liechtenstein, il FOTR di 9,0/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Maturità cyber (8,6/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

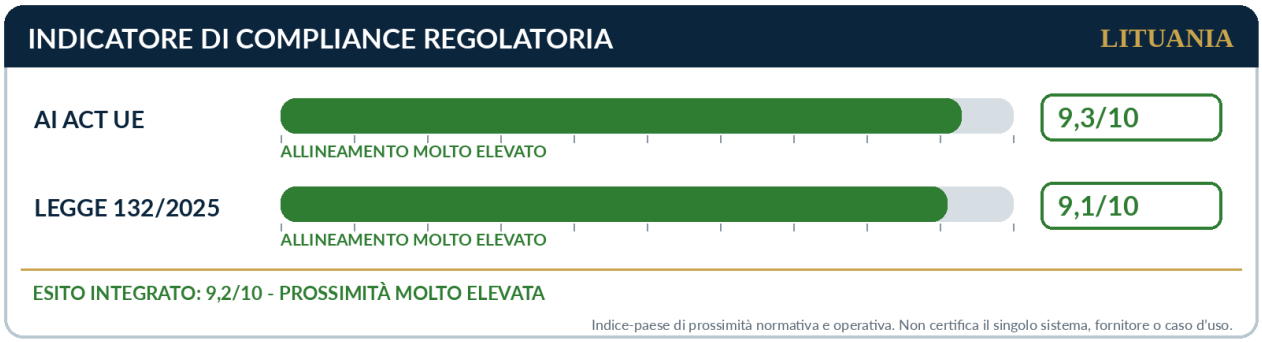
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Liechtenstein: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Lituania

Posizione FOTR	26	Area	Europa	Subregione	Europa settentrionale e baltica
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,5	GCRI / 10	7,8	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Lituania, AI Act UE 9,3/10; legge 132/2025 9,1/10; esito integrato 9,2/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Per un operatore italiano, Lituania non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 90/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,8/10) e indice FOTR (8,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Lituania presenta un ecosistema digitale maturo, istituzioni generalmente prevedibili e una buona capacità di gestione degli incidenti. Il rischio residuo deriva soprattutto dalla concentrazione cloud, dalle dipendenze extraeuropee e dalla complessità delle filiere software.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	89,2% / 27,8 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 98.553 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	91,1 / 88,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	92,9/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	69,0/100 - rank 29	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (90/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 7,4 / 4,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Lituania, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Lituania le evidenze principali sono GTMI 88,9/100, EGDI 91,1/100, GCI 92,9/100, AI readiness 69,0/100. La dimensione più robusta è maturità infrastrutturale (9,1/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,3/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Lituania è 9,1/10. La base statistica rileva utenti Internet pari al 89,2% nel 2024; 27,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 98.553 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Lituania al posto 29 con un valore medio di 69,0/100; il pilastro migliore è governance (91,7/100), quello più debole è sviluppo e diffusione (45,6/100). Il GTMI 2025 è 88,9/100. Il punteggio S2 è 7,4/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Lituania è valutata sufficiente ma disomogenea, con S3 pari a 7,7/10. Le evidenze disponibili comprendono indice UN di capitale umano 88,6/100, sviluppo e diffusione dell'IA 45,6/100, penetrazione Internet 89,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Lituania ottiene S4 6,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Lituania, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Lituania è S5 8,7/10. La base ITU registra ITU GCI 92,9/100, Tier 2 - avanzato; il pilastro relativamente più debole è organizzazione (17,1/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (90/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, Law on Legal Protection of Personal Data e disciplina nazionale di cybersicurezza/NIS2.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	6,0
Reti criminali	4,5	Attori incorporati nello Stato	4,0
Attori stranieri	4,5	Attori del settore privato	4,0
Resilienza complessiva	7,4	Cooperazione internazionale	8,5
Politiche e norme nazionali	7,5	Forze dell'ordine	7,5
Antiriciclaggio	6,5	Prevenzione	6,5
Supporto vittime e testimoni	7,0	Rischio operativo FOTR-CY	4,5 - MODERATO

Sintesi del rischio cybercrime. Lituania presenta un'esposizione stimata moderata (4,5/10): reati cyber-dipendenti 5,5/10, crimini finanziari 6,0/10 e resilienza 7,4/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (4,5/10) e attori stranieri (4,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Lituania assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Lituania, la resilienza complessiva è intermedia (7,4/10); la cooperazione internazionale è robusta (8,5/10), le politiche e norme nazionali sono robuste (7,5/10) e la capacità delle forze dell'ordine è robusta (7,5/10). Completano il quadro antiriciclaggio 6,5/10, prevenzione 6,5/10 e supporto a vittime e testimoni 7,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Lituania, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Lituania. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Lituania, In Lituania le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Lituania, Il livello governativo di Lituania presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Lituania, Sul piano militare e dual-use, Lituania mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Lituania, GDPR, Law on Legal Protection of Personal Data e disciplina nazionale di cybersicurezza/NIS2. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Lituania, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,5/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,1	7,4	7,7	6,3	8,7	7,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,0	7,7	7,7	9,2	7,8	9,5

Il GCRI di Lituania è 7,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,5/10), mentre il più basso è Maturità cyber (7,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Lituania, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Lituania, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Lituania, Dal punto di vista italiano, Lituania rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Lituania, il FOTR di 8,5/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Maturità cyber (7,7/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

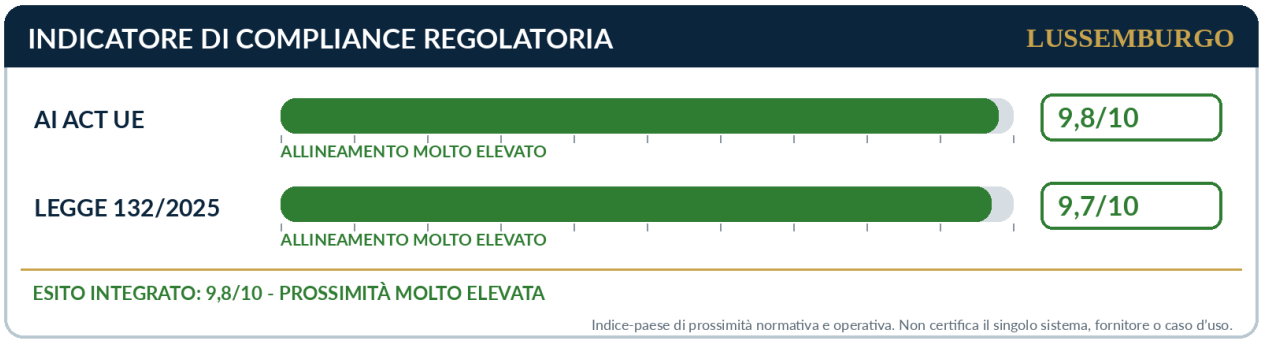
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Lituania: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Lussemburgo

Posizione FOTR	9	Area	Europa	Subregione	Europa occidentale e centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	9,1	GCRI / 10	8,0	Classe operativa	Affidabilità molto alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Lussemburgo, AI Act UE 9,8/10; legge 132/2025 9,7/10; esito integrato 9,8/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Lussemburgo è stato membro delle nazioni unite collocato in Europa occidentale e centrale. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 97/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (9,1/10) supera il GCRI tecnico (8,0/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Lussemburgo presenta un ecosistema digitale maturo, istituzioni generalmente prevedibili e una buona capacità di gestione degli incidenti. Il rischio residuo deriva soprattutto dalla concentrazione cloud, dalle dipendenze extraeuropee e dalla complessità delle filiere software.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	99,1% / 40,3 per 100	2025/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 58.438 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	84,7 / 78,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	98,7/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	68,1/100 - rank 33	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (97/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 7,5 / 3,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Lussemburgo, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Lussemburgo le evidenze principali sono GTMI 78,0/100, EGDI 84,7/100, GCI 98,7/100, AI readiness 68,1/100. La dimensione più robusta è maturità infrastrutturale (9,9/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,4/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Lussemburgo è 9,9/10. La base statistica rileva utenti Internet pari al 99,1% nel 2025; 40,3 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 58.438 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Lussemburgo al posto 33 con un valore medio di 68,1/100; il pilastro migliore è governance (81,5/100), quello più debole è sviluppo e diffusione (46,3/100). Il GTMI 2025 è 78,0/100. Il punteggio S2 è 7,0/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Lussemburgo è valutata sufficiente ma disomogenea, con S3 pari a 7,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 79,5/100, sviluppo e diffusione dell'IA 46,3/100, penetrazione Internet 99,1%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Lussemburgo ottiene S4 6,4/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open

source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Lussemburgo, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario, luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,4/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Lussemburgo è S5 9,3/10. La base ITU registra ITU GCI 98,7/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure tecniche (19,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (97/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, legge nazionale del 2018 e disciplina CSSF/settoriale; piena applicazione del quadro UE, incluso DORA per il finanziario.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	7,0
Reti criminali	2,0	Attori incorporati nello Stato	1,0
Attori stranieri	5,5	Attori del settore privato	4,0
Resilienza complessiva	7,5	Cooperazione internazionale	9,0
Politiche e norme nazionali	7,5	Forze dell'ordine	7,0
Antiriciclaggio	5,5	Prevenzione	7,5
Supporto vittime e testimoni	7,5	Rischio operativo FOTR-CY	3,9 - MODERATO

Rischio criminale connesso alle tecnologie. In Lussemburgo il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 3,9/10, livello moderato. I reati che dipendono direttamente da sistemi informatici raggiungono 4,5/10; le frodi e i reati finanziari 7,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (5,5/10) e attori del settore privato (4,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Lussemburgo assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Lussemburgo, la resilienza complessiva è robusta (7,5/10); la cooperazione internazionale è robusta (9,0/10), le politiche e norme nazionali sono robuste (7,5/10) e la capacità delle forze dell'ordine è intermedia (7,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 7,5/10 e supporto a vittime e testimoni 7,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Lussemburgo, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Lussemburgo. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Lussemburgo, In Lussemburgo le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Lussemburgo, Il livello governativo di Lussemburgo presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Lussemburgo, Sul piano militare e dual-use, Lussemburgo mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Lussemburgo, GDPR, legge nazionale del 2018 e disciplina CSSF/settoriale; piena applicazione del quadro UE, incluso DORA per il finanziario. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Lussemburgo, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 10,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,9	7,0	7,2	6,4	9,3	8,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,8	8,5	8,2	9,9	8,6	10,0

Il GCRI di Lussemburgo è 8,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 9,1/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (10,0/10), mentre il più basso è Trasparenza istituzionale (8,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Basso	Basso	Basso

La matrice applica il FOTR di 9,1/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Lussemburgo, la matrice non individua ambiti ad alto rischio; 6 categorie risultano basse o medio-basse, ferma la verifica del singolo progetto. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Lussemburgo, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Lussemburgo, Dal punto di vista italiano, Lussemburgo rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Lussemburgo, il FOTR di 9,1/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (8,2/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

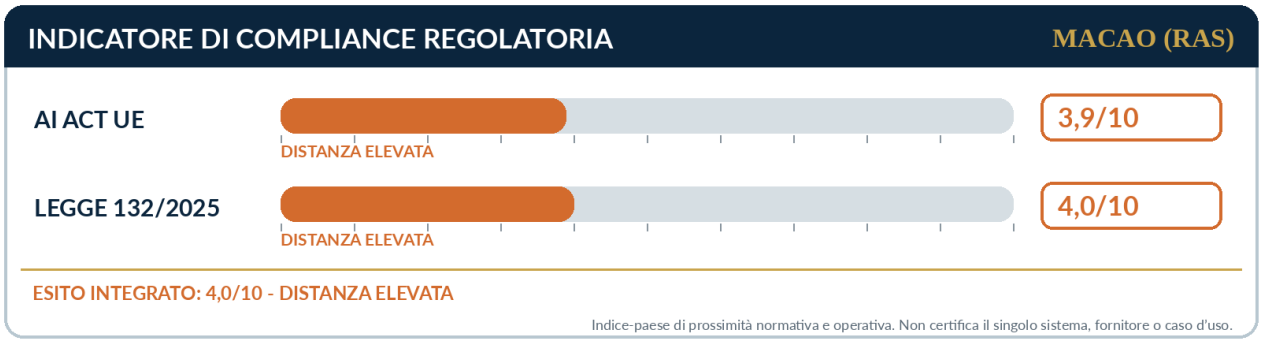
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Lussemburgo: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Macao (RAS)

Posizione FOTR	174	Area	Asia	Subregione	Asia orientale
Status	Regione amministrativa speciale della Cina	Confidenza Celeborn Intelligence	Media	Copertura dati	4/7 famiglie
FOTR / 10	4,0	GCRI / 10	4,8	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Macao (RAS), AI Act UE 3,9/10; legge 132/2025 4,0/10; esito integrato 4,0/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Nel quadro di Asia, Macao (RAS) presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Per questa entità non è disponibile un indicatore Freedom in the World direttamente comparabile; l'assenza di copertura viene trattata come limite informativo e non come prova automatica di rischio. GCRI tecnico (4,8/10) e indice FOTR (4,0/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Macao (RAS) presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	89,8% / 29,9 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 6.587 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	n.d. / 40,1	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	n.d./100 - n.d.	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	n.d./100 - rank n.d.	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / n.d.	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	8,1 / 6,1 / 6,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Macao (RAS), n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 4/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Macao (RAS) le evidenze principali sono GTMI 40,1/100. La dimensione più robusta è maturità infrastrutturale (8,5/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (2,3/10). Sono disponibili 4 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata media. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Macao (RAS) è 8,5/10. La base statistica rileva utenti Internet pari al 89,8% nel 2024; 29,9 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 6.587 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Per Macao (RAS) non è disponibile un profilo Oxford Insights direttamente attribuibile; l'adozione di IA è quindi valutata attraverso GovTech, servizi online, infrastrutture e fonti qualitative. Il GTMI 2025 è 40,1/100. Il punteggio S2 è 4,0/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Macao (RAS) è valutata fragile, con S3 pari a 2,3/10. Le evidenze disponibili comprendono penetrazione Internet 89,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Macao (RAS) ottiene S4 4,7/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Macao (RAS), Prevalenza di fornitori cinesi e operatori regionali, con mercato locale ristretto. L'impatto sulla valutazione è misurato da S4=4,7/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Macao (RAS) è S5 4,5/10. La base ITU registra GCI non disponibile in forma comparabile. Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è n.d.. Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Personal Data Protection Act locale e disciplina della RAS, con interdipendenza normativa e operativa dalla Cina; trasferimenti sensibili da sottoporre a controllo rafforzato.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	8,1	Crimini finanziari	7,1
Reti criminali	6,9	Attori incorporati nello Stato	5,6
Attori stranieri	2,6	Attori del settore privato	6,1
Resilienza complessiva	6,1	Cooperazione internazionale	7,1
Politiche e norme nazionali	7,4	Forze dell'ordine	6,8
Antiriciclaggio	6,8	Prevenzione	6,4
Supporto vittime e testimoni	4,8	Rischio operativo FOTR-CY	6,1 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Macao (RAS) presenta un'esposizione stimata significativa (6,1/10): reati cyber-dipendenti 8,1/10, crimini finanziari 7,1/10 e resilienza 6,1/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (6,9/10) e attori del settore privato (6,1/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Macao (RAS) assumono particolare rilevanza compromissioni della supply chain, sottrazione di proprietà intellettuale, furto di cripto-attività, phishing mirato, abuso di identità digitali e intrusioni persistenti contro industria e amministrazioni. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Macao (RAS), la resilienza complessiva è intermedia (6,1/10); la cooperazione internazionale è intermedia (7,1/10), le politiche e norme nazionali sono intermedie (7,4/10) e la capacità delle forze dell'ordine è intermedia (6,8/10). Completano il quadro antiriciclaggio 6,8/10, prevenzione 6,4/10 e supporto a vittime e testimoni 4,8/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Macao (RAS), il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE. Poiché l'entità non dispone di una serie nazionale GI-TOC autonoma, i valori derivano da un proxy Celeborn Intelligence ponderato su Cina 75%, Singapore 25%; la confidenza deve pertanto essere considerata inferiore e la decisione resa più prudente.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; proxy Celeborn Intelligence ponderato su Cina 75%, Singapore 25%. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Macao (RAS), In Macao (RAS) le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Macao (RAS), Il livello governativo di Macao (RAS) presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Macao (RAS), Sul piano militare e dual-use, Macao (RAS) mostra forte ruolo statale e integrazione con filiere cinesi o nazionali, con limitata trasparenza esterna. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Macao (RAS), Personal Data Protection Act locale e disciplina della RAS, con interdipendenza normativa e operativa dalla Cina; trasferimenti sensibili da sottoporre a controllo rafforzato. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Macao (RAS), Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 3,0/10 e il rischio sui dati personali è Alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,5	4,0	2,3	4,7	4,5	4,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,0	5,8	2,3	4,0	5,0	3,0

Il GCRI di Macao (RAS) è 4,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (5,8/10), mentre il più basso è Trasparenza istituzionale (2,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Alto	Alto	Medio-alto	Alto	Medio-alto	Alto

La matrice applica il FOTR di 4,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Macao (RAS), 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Macao (RAS), sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Macao (RAS), Dal punto di vista italiano, Macao (RAS) rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Macao (RAS) ricade nella fascia di alto rischio (4,0/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

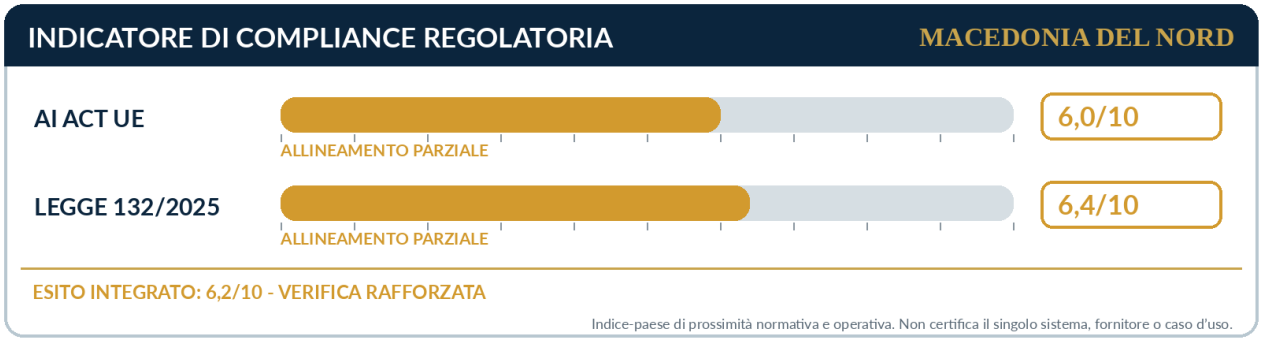
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Macao (RAS): World Development Indicators, valori più recenti disponibili 2022-2024; World Bank GovTech Maturity Index 2025; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Media con copertura 4/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Macedonia del Nord

Posizione FOTR	66	Area	Europa	Subregione	Europa sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	6,2	GCRI / 10	6,1	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Macedonia del Nord, AI Act UE 6,0/10; legge 132/2025 6,4/10; esito integrato 6,2/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Macedonia del Nord, situato in Europa sud-orientale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La collocazione nell'Alleanza Atlantica favorisce interoperabilità e cooperazione di sicurezza, senza equivalere automaticamente ad allineamento pieno sul diritto dei dati. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Cina, Russia, Turchia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 67/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,1/10) e indice FOTR (6,2/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il quadro di Macedonia del Nord è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	93,1% / 29,9 per 100	2025/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 2.068 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	70,7 / 76,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	65,9/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	38,5/100 - rank 107	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (67/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 5,3 / 5,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Macedonia del Nord, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Macedonia del Nord le evidenze principali sono GTMI 76,0/100, EGDI 70,7/100, GCI 65,9/100, AI readiness 38,5/100. La dimensione più robusta è maturità infrastrutturale (8,1/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (5,0/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Macedonia del Nord è 8,1/10. La base statistica rileva utenti Internet pari al 93,1% nel 2025; 29,9 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 2.068 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Macedonia del Nord al posto 107 con un valore medio di 38,5/100; il pilastro migliore è adozione pubblica (46,5/100), quello più debole è sviluppo e diffusione (24,9/100). Il GTMI 2025 è 76,0/100. Il punteggio S2 è 5,0/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Macedonia del Nord è valutata sufficiente ma disomogenea, con S3 pari a 5,3/10. Le evidenze disponibili comprendono indice UN di capitale umano 70,2/100, sviluppo e diffusione dell'IA 24,9/100, penetrazione Internet 93,1%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Macedonia del Nord ottiene S4 6,0/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Cina, Russia, Turchia; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Macedonia del Nord, Mercato multi-fornitore tra Unione europea, Stati Uniti, Turchia, Cina e, in alcuni segmenti, Russia; il peso relativo varia tra pubblico, telecomunicazioni e difesa. L'impatto sulla

valutazione è misurato da S4=6,0/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Macedonia del Nord è S5 6,3/10. La base ITU registra ITU GCI 65,9/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (8,9/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (67/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Quadro nazionale di protezione dati e cybersicurezza in progressivo allineamento all'acquis dell'Unione europea; la distanza tra legge formale, vigilanza e prassi deve essere verificata nel settore interessato.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	6,0
Reti criminali	6,0	Attori incorporati nello Stato	6,5
Attori stranieri	5,0	Attori del settore privato	5,0
Resilienza complessiva	5,3	Cooperazione internazionale	6,5
Politiche e norme nazionali	5,0	Forze dell'ordine	5,5
Antiriciclaggio	6,0	Prevenzione	5,5
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	5,5 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Macedonia del Nord presenta un'esposizione stimata significativa (5,5/10): reati cyber-dipendenti 5,5/10, crimini finanziari 6,0/10 e resilienza 5,3/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (6,5/10) e reti criminali (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Macedonia del Nord assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Macedonia del Nord, la resilienza complessiva è debole (5,3/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 5,5/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Macedonia del Nord, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Macedonia del Nord. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Macedonia del Nord, In Macedonia del Nord le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora

visibili. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Macedonia del Nord, Il livello governativo di Macedonia del Nord presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Macedonia del Nord, Sul piano militare e dual-use, Macedonia del Nord mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Macedonia del Nord, Quadro nazionale di protezione dati e cybersicurezza in progressivo allineamento all'acquis dell'Unione europea; la distanza tra legge formale, vigilanza e prassi deve essere verificata nel settore interessato. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Macedonia del Nord, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,2/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,1	5,0	5,3	6,0	6,3	6,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,7	6,0	5,4	8,3	5,7	5,2

Il GCRI di Macedonia del Nord è 6,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (8,3/10), mentre il più basso è Trasferibilità dati (5,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Macedonia del Nord, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Macedonia del Nord, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Macedonia del Nord, Dal punto di vista italiano, Macedonia del Nord rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Macedonia del Nord è indicata una cooperazione selettiva, coerente con il FOTR di 6,2/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasferibilità dati a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

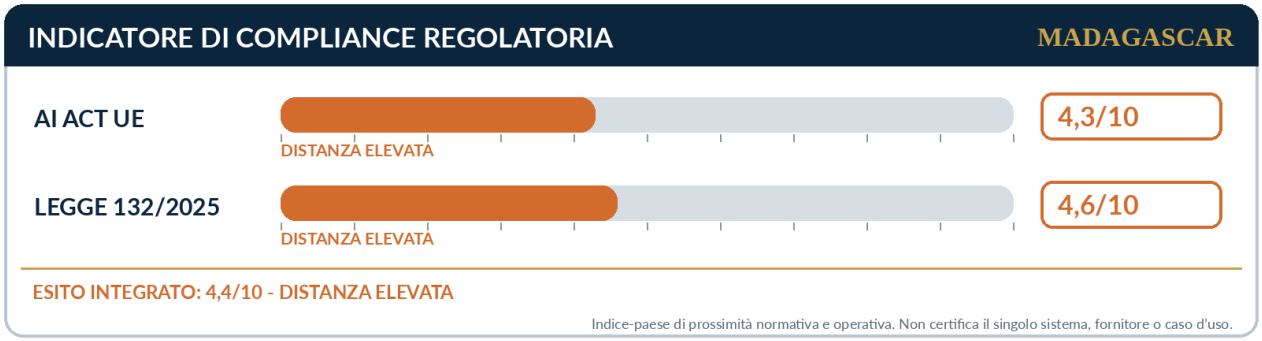
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Macedonia del Nord: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Madagascar

Posizione FOTR	149	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,5	GCRI / 10	3,2	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Madagascar, AI Act UE 4,3/10; legge 132/2025 4,6/10; esito integrato 4,4/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Per un operatore italiano, Madagascar non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 50/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (4,5/10) supera il GCRI tecnico (3,2/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Madagascar è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	18,7% / 0,1 per 100	2024/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	42,5% / 25 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	32,3 / 37,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	31,9/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	20,0/100 - rank 168	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (50/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 3,2 / 5,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Madagascar, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Madagascar le evidenze principali sono GTMI 37,8/100, EGDI 32,3/100, GCI 31,9/100, AI readiness 20,0/100. La dimensione più robusta è indipendenza della supply chain (4,4/10), mentre la criticità relativa riguarda maturità infrastrutturale (1,8/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Madagascar è 1,8/10. La base statistica rileva utenti Internet pari al 18,7% nel 2024; 0,1 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 42,5% nel 2024; 25 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Madagascar al posto 168 con un valore medio di 20,0/100; il pilastro migliore è adozione pubblica (30,9/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 37,8/100. Il punteggio S2 è 2,7/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Madagascar è valutata fragile, con S3 pari a 3,3/10. Le evidenze disponibili comprendono indice UN di capitale umano 41,4/100, sviluppo e diffusione dell'IA 11,9/100, penetrazione Internet 18,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Madagascar ottiene S4 4,4/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Madagascar, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre

ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,4/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Madagascar è S5 3,7/10. La base ITU registra ITU GCI 31,9/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (2,9/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (50/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	6,0
Reti criminali	6,0	Attori incorporati nello Stato	8,0
Attori stranieri	6,5	Attori del settore privato	5,5
Resilienza complessiva	3,2	Cooperazione internazionale	3,0
Politiche e norme nazionali	3,5	Forze dell'ordine	3,5
Antiriciclaggio	4,5	Prevenzione	4,0
Supporto vittime e testimoni	2,5	Rischio operativo FOTR-CY	5,2 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Madagascar presenta un'esposizione stimata significativa (5,2/10): reati cyber-dipendenti 2,0/10, crimini finanziari 6,0/10 e resilienza 3,2/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e attori stranieri (6,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Madagascar assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Madagascar, la resilienza complessiva è molto debole (3,2/10); la cooperazione internazionale è molto debole (3,0/10), le politiche e norme nazionali sono deboli (3,5/10) e la capacità delle forze dell'ordine è debole (3,5/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 4,0/10 e supporto a vittime e testimoni 2,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Madagascar, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Madagascar. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Madagascar, In Madagascar le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La

superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Madagascar, Il livello governativo di Madagascar presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Madagascar, Sul piano militare e dual-use, Madagascar mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Madagascar, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Madagascar, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 3,9/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
1,8	2,7	3,3	4,4	3,7	3,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,7	4,5	4,5	5,2	4,4	3,9

Il GCRI di Madagascar è 3,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,2/10), mentre il più basso è Trasferibilità dati (3,9/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Madagascar, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Madagascar, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Madagascar, Dal punto di vista italiano, Madagascar rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Madagascar ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

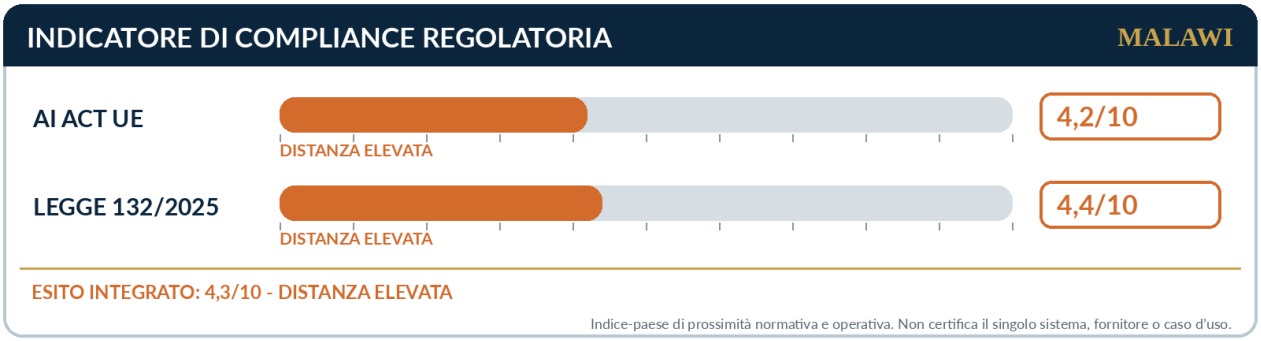
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Madagascar: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Malawi

Posizione FOTR	167	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	4,4	GCRI / 10	3,9	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Malawi, AI Act UE 4,2/10; legge 132/2025 4,4/10; esito integrato 4,3/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Malawi è stato membro delle nazioni unite collocato in Africa orientale. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 68/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (3,9/10) e indice FOTR (4,4/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per Malawi non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	19,0% / 0,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	15,6% / 32 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	37,5 / 32,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	80,4/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	24,9/100 - rank 149	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	61/100 - Parzialmente libero / Libero (68/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Firmatario/invitato	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,5 / 4,4 / 4,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Malawi, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Malawi le evidenze principali sono GTMI 32,8/100, EGDI 37,5/100, GCI 80,4/100, AI readiness 24,9/100. La dimensione più robusta è postura di sicurezza cyber (6,6/10), mentre la criticità relativa riguarda maturità infrastrutturale (1,7/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Malawi è 1,7/10. La base statistica rileva utenti Internet pari al 19,0% nel 2024; 0,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 15,6% nel 2024; 32 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Malawi al posto 149 con un valore medio di 24,9/100; il pilastro migliore è governance (37,9/100), quello più debole è adozione pubblica (5,8/100). Il GTMI 2025 è 32,8/100. Il punteggio S2 è 2,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Malawi è valutata fragile, con S3 pari a 3,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 47,5/100, sviluppo e diffusione dell'IA 18,6/100, penetrazione Internet 19,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Malawi ottiene S4 4,4/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Malawi, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,4/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Malawi è S5 6,6/10. La base ITU registra ITU GCI 80,4/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (12,3/20). Freedom on the Net è 61/100 - Parzialmente libero, mentre Freedom in the World è Libero (68/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Firmatario/invitato. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,5	Crimini finanziari	7,0
Reti criminali	4,5	Attori incorporati nello Stato	4,0
Attori stranieri	5,5	Attori del settore privato	4,0
Resilienza complessiva	4,4	Cooperazione internazionale	5,5
Politiche e norme nazionali	5,5	Forze dell'ordine	3,5
Antiriciclaggio	5,0	Prevenzione	4,0
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	4,6 - MODERATO

Pressione del crimine digitale. Il profilo di Malawi restituisce un rischio FOTR-CY di 4,6/10 (moderato). La componente cyber-dipendente vale 2,5/10 e quella finanziaria 7,0/10; la risposta sistemica è valutata debole, con resilienza media di 4,4/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (5,5/10) e reti criminali (4,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Malawi assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Malawi, la resilienza complessiva è debole (4,4/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è debole (3,5/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Malawi, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Malawi. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Malawi, In Malawi le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Malawi, Il livello governativo di Malawi presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Malawi, Sul piano militare e dual-use, Malawi mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Malawi, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Firmatario/invitato; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Malawi, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,1/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
1,7	2,9	3,8	4,4	6,6	3,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,4	4,7	4,0	5,1	4,1	4,1

Il GCRI di Malawi è 3,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,1/10), mentre il più basso è Trasparenza istituzionale (4,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Malawi, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Malawi, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Malawi, Dal punto di vista italiano, Malawi rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Malawi ricade nella fascia di alto rischio (4,4/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.
Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

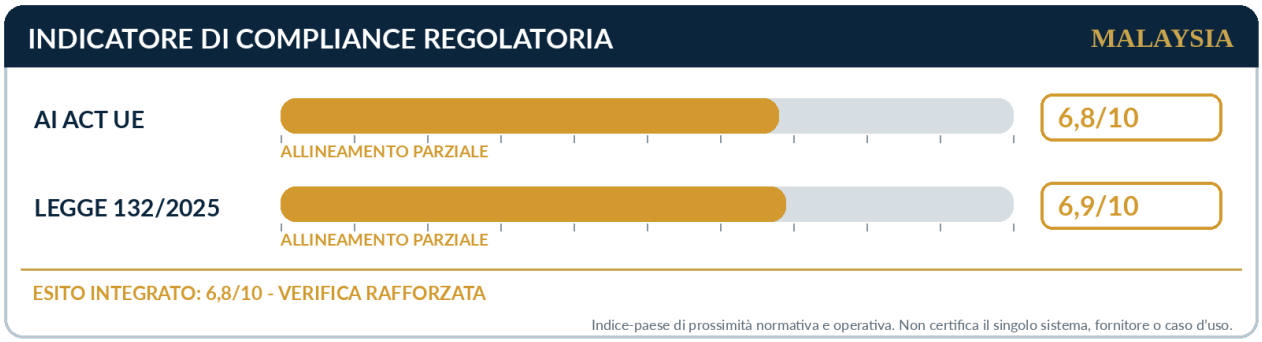
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Malawi: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Malaysia

Posizione FOTR	52	Area	Asia	Subregione	Asia sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	6,8	GCRI / 10	7,6	Classe operativa	Affidabilità favorevole ma condizionata

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Malaysia, AI Act UE 6,8/10; legge 132/2025 6,9/10; esito integrato 6,8/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Asia, Malaysia presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 53/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,6/10) e indice FOTR (6,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. In Malaysia la trasformazione digitale procede più rapidamente dell'uniformità regolatoria e operativa. Gli investimenti devono essere accompagnati da audit, clausole di uscita e gestione locale del rischio.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	98,0% / 13,5 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 7.475 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	81,1 / 84,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	98,8/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	63,0/100 - rank 38	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	60/100 - Parzialmente libero / Parzialmente libero (53/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Firmatario/invitato	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	8,0 / 5,7 / 6,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Malaysia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Malaysia le evidenze principali sono GTMI 84,8/100, EGDI 81,1/100, GCI 98,8/100, AI readiness 63,0/100. La dimensione più robusta è maturità infrastrutturale (8,4/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (6,8/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Malaysia è 8,4/10. La base statistica rileva utenti Internet pari al 98,0% nel 2024; 13,5 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 7.475 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Malaysia al posto 38 con un valore medio di 63,0/100; il pilastro migliore è politiche pubbliche (80,5/100), quello più debole è resilienza (38,3/100). Il GTMI 2025 è 84,8/100. Il punteggio S2 è 6,8/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Malaysia è valutata sufficiente ma disomogenea, con S3 pari a 6,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 71,9/100, sviluppo e diffusione dell'IA 55,4/100, penetrazione Internet 98,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Malaysia ottiene S4 7,7/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Stati Uniti; l'indicatore di indipendenza disponibile è 8,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Malaysia, Ecosistema multi-fornitore asiatico e statunitense, con significativa capacità produttiva locale. L'impatto sulla valutazione è misurato da S4=7,7/10 e dal proxy di indipendenza 8,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Malaysia è S5 8,2/10. La base ITU registra ITU GCI 98,8/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è organizzazione (18,8/20). Freedom on the Net è 60/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (53/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Firmatario/invitato. Quadro normativo sintetico: Personal Data Protection Act 2010 e successive riforme, Cyber Security Act e disciplina settoriale; esclusioni e poteri pubblici richiedono analisi mirata.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	8,0	Crimini finanziari	8,0
Reti criminali	6,0	Attori incorporati nello Stato	7,0
Attori stranieri	7,0	Attori del settore privato	7,0
Resilienza complessiva	5,7	Cooperazione internazionale	7,0
Politiche e norme nazionali	7,5	Forze dell'ordine	5,5
Antiriciclaggio	6,0	Prevenzione	6,0
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	6,7 - ALTO

Pressione del crimine digitale. Il profilo di Malaysia restituisce un rischio FOTR-CY di 6,7/10 (alto). La componente cyber-dipendente vale 8,0/10 e quella finanziaria 8,0/10; la risposta sistemica è valutata intermedia, con resilienza media di 5,7/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,0/10) e attori stranieri (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Malaysia assumono particolare rilevanza centri organizzati di truffa, frodi d'investimento e sentimentali, phishing multicanale, batterie di schede SIM, conti prestanome, riciclaggio in cripto-attività e compromissione di servizi esternalizzati. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Malaysia, la resilienza complessiva è intermedia (5,7/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono robuste (7,5/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 6,0/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Malaysia, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; controllo della filiera contro esposizione a complessi organizzati per truffe telematiche, call center coercitivi e conti prestanome; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Malaysia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Malaysia, In Malaysia le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Malaysia, Il livello governativo di Malaysia presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Malaysia, Sul piano militare e dual-use, Malaysia mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Malaysia, Personal Data Protection Act 2010 e successive riforme, Cyber Security Act e disciplina settoriale; esclusioni e poteri pubblici richiedono analisi mirata. Lo stato rispetto alla Convenzione di Budapest è: Firmatario/invitato; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Malaysia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 6,3/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,4	6,8	6,8	7,7	8,2	7,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,9	7,3	6,4	6,9	7,3	6,3

Il GCRI di Malaysia è 7,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (7,3/10), mentre il più basso è Trasferibilità dati (6,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio-basso	Medio	Medio	Medio

La matrice applica il FOTR di 6,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Malaysia, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Malaysia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Malaysia, Dal punto di vista italiano, Malaysia rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Malaysia è favorevole ma condizionata: il valore FOTR di 6,8/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Trasferibilità dati.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

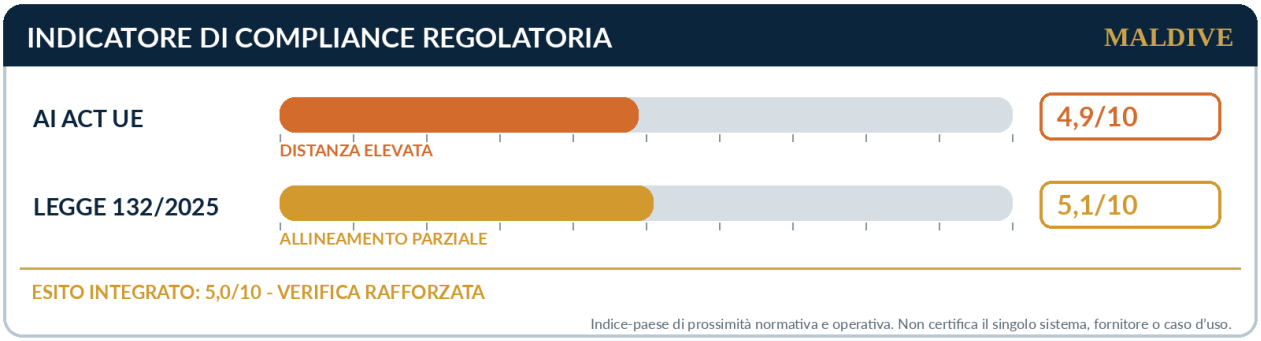
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Malaysia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Maldive

Posizione FOTR	133	Area	Asia	Subregione	Asia meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,1	GCRI / 10	4,5	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Maldive, AI Act UE 4,9/10; legge 132/2025 5,1/10; esito integrato 5,0/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Maldive, situato in Asia meridionale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 41/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (4,5/10) e indice FOTR (5,1/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Maldive è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	85,2% / 19,6 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 1.330 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	67,5 / 35,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	14,8/100 - Tier 5 - capacità iniziali	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	25,1/100 - rank 143	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (41/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,5 / 4,0 / 4,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Maldive, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Maldive le evidenze principali sono GTMI 35,9/100, EGDI 67,5/100, GCI 14,8/100, AI readiness 25,1/100. La dimensione più robusta è maturità infrastrutturale (7,6/10), mentre la criticità relativa riguarda postura di sicurezza cyber (2,8/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Maldive è 7,6/10. La base statistica rileva utenti Internet pari al 85,2% nel 2024; 19,6 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 1.330 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Maldive al posto 143 con un valore medio di 25,1/100; il pilastro migliore è infrastrutture IA (39,4/100), quello più debole è politiche pubbliche (8,0/100). Il GTMI 2025 è 35,9/100. Il punteggio S2 è 3,3/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Maldive è valutata fragile, con S3 pari a 4,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 61,3/100, sviluppo e diffusione dell'IA 18,8/100, penetrazione Internet 85,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Maldive ottiene S4 4,2/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Maldive, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo

societario e subfornitura. L'impatto sulla valutazione è misurato da S4=4,2/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Maldive è S5 2,8/10. La base ITU registra ITU GCI 14,8/100, Tier 5 - capacità iniziali; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (41/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,5	Crimini finanziari	4,0
Reti criminali	6,0	Attori incorporati nello Stato	5,5
Attori stranieri	4,5	Attori del settore privato	4,0
Resilienza complessiva	4,0	Cooperazione internazionale	5,5
Politiche e norme nazionali	5,0	Forze dell'ordine	4,0
Antiriciclaggio	3,5	Prevenzione	3,5
Supporto vittime e testimoni	2,5	Rischio operativo FOTR-CY	4,8 - MODERATO

Rischio criminale connesso alle tecnologie. In Maldive il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 4,8/10, livello moderato. I reati che dipendono direttamente da sistemi informatici raggiungono 3,5/10; le frodi e i reati finanziari 4,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (6,0/10) e attori incorporati nello Stato (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Maldive assumono particolare rilevanza compromissione delle caselle di posta aziendale, frodi da call center, abuso di portafogli digitali mobili, identità sintetiche, ransomware, phishing bancario e triangolazioni transfrontaliere dei proventi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Maldive, la resilienza complessiva è debole (4,0/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 3,5/10 e supporto a vittime e testimoni 2,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Maldive, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Maldive. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Maldive, In Maldive le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Maldive, Il livello governativo di Maldive presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Maldive, Sul piano militare e dual-use, Maldive mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Maldive, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Maldive, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,7/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,6	3,3	4,4	4,2	2,8	4,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,1	5,3	5,1	5,4	5,1	4,7

Il GCRI di Maldive è 4,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,1/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,4/10), mentre il più basso è Trasferibilità dati (4,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 5,1/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Maldive, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Maldive, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Maldive, Dal punto di vista italiano, Maldive rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Maldive è indicata una cooperazione selettiva, coerente con il FOTR di 5,1/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.
Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

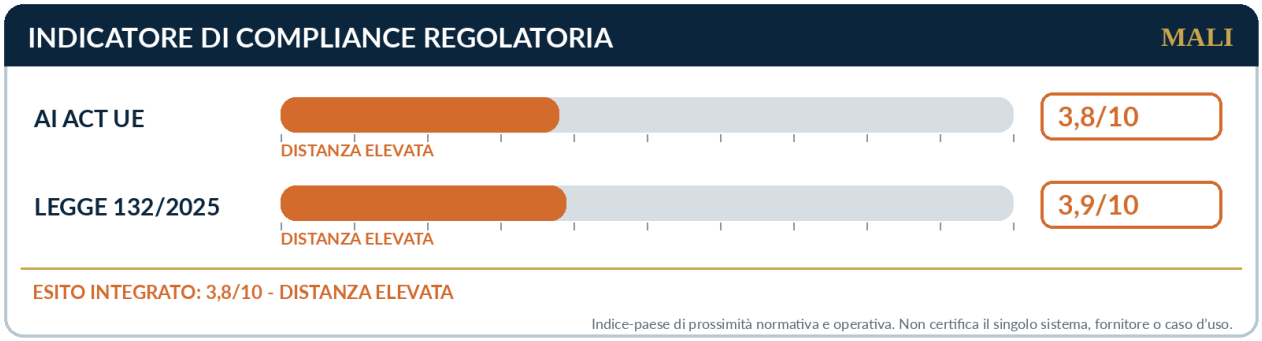
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Maldive: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Mali

Posizione FOTR	180	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	3,8	GCRI / 10	2,7	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Mali, AI Act UE 3,8/10; legge 132/2025 3,9/10; esito integrato 3,8/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Per un operatore italiano, Mali non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 21/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (3,8/10) supera il GCRI tecnico (2,7/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Mali presenta un livello di rischio elevato per cooperazione digitale, dovuto a limitata trasparenza, poteri pubblici, instabilità o dipendenze tecnologiche. Le attività dovrebbero escludere dati sensibili e asset strategici.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	36,8% / 0,8 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	49,5% / 21 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	30,1 / 32,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	29,5/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	22,3/100 - rank 152	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (21/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,0 / 2,1 / 6,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Mali, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Mali le evidenze principali sono GTMI 32,6/100, EGDI 30,1/100, GCI 29,5/100, AI readiness 22,3/100. La dimensione più robusta è indipendenza della supply chain (3,6/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (2,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Mali è 2,8/10. La base statistica rileva utenti Internet pari al 36,8% nel 2024; 0,8 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 49,5% nel 2024; 21 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Mali al posto 152 con un valore medio di 22,3/100; il pilastro migliore è governance (38,0/100), quello più debole è politiche pubbliche (4,0/100). Il GTMI 2025 è 32,6/100. Il punteggio S2 è 2,6/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Mali è valutata fragile, con S3 pari a 2,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 12,5/100, sviluppo e diffusione dell'IA 18,1/100, penetrazione Internet 36,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Mali ottiene S4 3,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Mali, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=3,6/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Mali è S5 2,3/10. La base ITU registra ITU GCI 29,5/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è sviluppo delle capacità (0,8/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (21/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,0	Crimini finanziari	7,0
Reti criminali	6,5	Attori incorporati nello Stato	8,0
Attori stranieri	6,0	Attori del settore privato	4,0
Resilienza complessiva	2,1	Cooperazione internazionale	3,0
Politiche e norme nazionali	2,5	Forze dell'ordine	2,0
Antiriciclaggio	2,5	Prevenzione	2,0
Supporto vittime e testimoni	1,5	Rischio operativo FOTR-CY	6,5 - ALTO

Quadro criminale digitale. Per Mali, l'indice operativo FOTR-CY è 6,5/10, classe alta. Il mercato dei reati cyber-dipendenti è intermedio (4,0/10), mentre i crimini finanziari sono elevati (7,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e reti criminali (6,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Mali assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Mali, la resilienza complessiva è molto debole (2,1/10); la cooperazione internazionale è molto debole (3,0/10), le politiche e norme nazionali sono molto deboli (2,5/10) e la capacità delle forze dell'ordine è molto debole (2,0/10). Completano il quadro antiriciclaggio 2,5/10, prevenzione 2,0/10 e supporto a vittime e testimoni 1,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Mali, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Mali. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Mali, In Mali le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Mali, Il livello governativo di Mali presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Mali, Sul piano militare e dual-use, Mali mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Mali, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Mali, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 3,1/10 e il rischio sui dati personali è Alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
2,8	2,6	2,1	3,6	2,3	2,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,7	3,3	3,6	4,8	3,1	3,1

Il GCRI di Mali è 2,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 3,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (4,8/10), mentre il più basso è Supply chain (3,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Alto	Medio-alto	Alto	Alto	Alto	Alto

La matrice applica il FOTR di 3,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Mali, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Mali, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Mali, Dal punto di vista italiano, Mali rientra nella classe «Rischio alto»: cooperazione eccezionale e ad alto controllo, subordinata a assenza di dati sensibili, verifica sanzionatoria, autorizzazioni interne e impossibilità di accesso ai sistemi strategici. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Mali ricade nella fascia di alto rischio (3,8/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

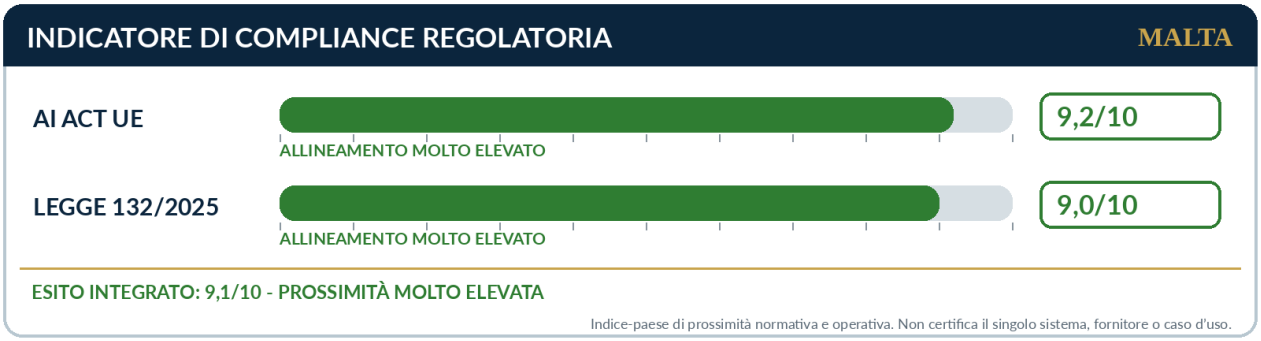
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Mali: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Malta

Posizione FOTR	30	Area	Europa	Subregione	Europa meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,3	GCRI / 10	7,7	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Malta, AI Act UE 9,2/10; legge 132/2025 9,0/10; esito integrato 9,1/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Malta è stato membro delle nazioni unite collocato in Europa meridionale. L'appartenenza all'Unione europea inserisce il Paese nel mercato digitale unico, nel sistema GDPR e nelle principali discipline comuni su cybersicurezza, dati e intelligenza artificiale. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 88/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,7/10) e indice FOTR (8,3/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Malta offre condizioni favorevoli alla cooperazione tecnologica, con capacità istituzionali e cyber generalmente robuste. Restano differenze settoriali che rendono necessaria una verifica preventiva proporzionata ai dati e alla criticità del progetto.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	93,9% / 44,5 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 4.507 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	88,9 / 84,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	93,0/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	65,5/100 - rank 39	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (88/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 5,1 / 6,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Malta, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Malta le evidenze principali sono GTMI 84,9/100, EGDI 88,9/100, GCI 93,0/100, AI readiness 65,5/100. La dimensione più robusta è maturità infrastrutturale (9,4/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Malta è 9,4/10. La base statistica rileva utenti Internet pari al 93,9% nel 2024; 44,5 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 4.507 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Malta al posto 39 con un valore medio di 65,5/100; il pilastro migliore è governance (87,8/100), quello più debole è sviluppo e diffusione (44,2/100). Il GTMI 2025 è 84,9/100. Il punteggio S2 è 7,1/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Malta è valutata sufficiente ma disomogenea, con S3 pari a 7,3/10. Le evidenze disponibili comprendono indice UN di capitale umano 81,6/100, sviluppo e diffusione dell'IA 44,2/100, penetrazione Internet 93,9%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Malta ottiene S4 5,9/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Malta, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=5,9/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Malta è S5 8,8/10. La base ITU registra ITU GCI 93,0/100, Tier 2 - avanzato; il pilastro relativamente più debole è sviluppo delle capacità (16,8/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (88/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, Data Protection Act e quadro nazionale cyber; applicazione dei regolamenti digitali UE.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	8,0
Reti criminali	7,0	Attori incorporati nello Stato	7,5
Attori stranieri	5,0	Attori del settore privato	6,5
Resilienza complessiva	5,1	Cooperazione internazionale	7,0
Politiche e norme nazionali	6,0	Forze dell'ordine	5,0
Antiriciclaggio	4,0	Prevenzione	4,0
Supporto vittime e testimoni	7,0	Rischio operativo FOTR-CY	6,0 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (5,5/10), criminalità finanziaria (8,0/10) e resilienza (5,1/10) colloca Malta in una fascia di rischio significativo, pari a 6,0/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,5/10) e reti criminali (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Malta assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Malta, la resilienza complessiva è debole (5,1/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 7,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Malta, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Malta. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Malta, In Malta le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Malta, Il livello governativo di Malta presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Malta, Sul piano militare e dual-use, Malta mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Malta, GDPR, Data Protection Act e quadro nazionale cyber; applicazione dei regolamenti digitali UE. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Malta, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,1/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,4	7,1	7,3	5,9	8,8	7,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,1	7,8	7,8	8,9	7,0	9,1

Il GCRI di Malta è 7,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,3/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (9,1/10), mentre il più basso è Supply chain (7,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,3/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Malta, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Malta, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Malta, Dal punto di vista italiano, Malta rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Malta, il FOTR di 8,3/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (7,0/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

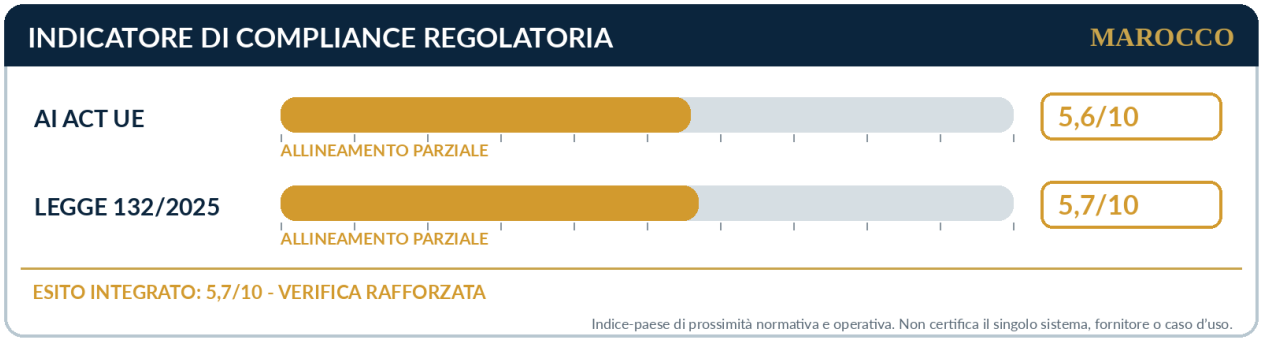
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Malta: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Marocco

Posizione FOTR	100	Area	Africa	Subregione	Africa settentrionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,7	GCRI / 10	6,1	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Marocco, AI Act UE 5,6/10; legge 132/2025 5,7/10; esito integrato 5,7/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Marocco presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 37/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,1/10) e indice FOTR (5,7/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. In Marocco la trasformazione digitale procede più rapidamente dell'uniformità regolatoria e operativa. Gli investimenti devono essere accompagnati da audit, clausole di uscita e gestione locale del rischio.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	91,2% / 7,3 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 577 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	68,4 / 51,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	97,5/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	42,6/100 - rank 86	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	54/100 - Parzialmente libero / Parzialmente libero (37/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 4,7 / 5,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Marocco, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Marocco le evidenze principali sono GTMI 51,6/100, EGDI 68,4/100, GCI 97,5/100, AI readiness 42,6/100. La dimensione più robusta è postura di sicurezza cyber (7,6/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,7/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Marocco è 7,4/10. La base statistica rileva utenti Internet pari al 91,2% nel 2024; 7,3 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 577 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Marocco al posto 86 con un valore medio di 42,6/100; il pilastro migliore è governance (78,8/100), quello più debole è politiche pubbliche (23,0/100). Il GTMI 2025 è 51,6/100. Il punteggio S2 è 4,7/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Marocco è valutata sufficiente ma disomogenea, con S3 pari a 5,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 60,8/100, sviluppo e diffusione dell'IA 30,8/100, penetrazione Internet 91,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Marocco ottiene S4 5,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Marocco, Prevalenza europea, statunitense e cinese, con crescente capacità locale e integrazione con filiere UE. L'impatto sulla valutazione è misurato da S4=5,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Marocco è S5 7,6/10. La base ITU registra ITU GCI 97,5/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure tecniche (18,1/20). Freedom on the Net è 54/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (37/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge 09-08 sulla protezione dei dati e disciplina DGSSI; cooperazione con l'Europa significativa, ma trasferimenti da strutturare con garanzie.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	7,5
Reti criminali	7,0	Attori incorporati nello Stato	7,5
Attori stranieri	5,5	Attori del settore privato	4,5
Resilienza complessiva	4,7	Cooperazione internazionale	6,0
Politiche e norme nazionali	6,5	Forze dell'ordine	5,5
Antiriciclaggio	4,0	Prevenzione	4,0
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	5,8 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Marocco restituisce un rischio FOTR-CY di 5,8/10 (significativo). La componente cyber-dipendente vale 4,5/10 e quella finanziaria 7,5/10; la risposta sistemica è valutata debole, con resilienza media di 4,7/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,5/10) e reti criminali (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Marocco assumono particolare rilevanza phishing e credential theft, ransomware, frodi d'investimento, attacchi a energia e servizi pubblici, abuso di cripto-attività e campagne che possono combinare profitto, spionaggio e pressione politica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Marocco, la resilienza complessiva è debole (4,7/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Marocco, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Marocco. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Marocco, In Marocco le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio

comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Marocco, Il livello governativo di Marocco presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Marocco, Sul piano militare e dual-use, Marocco mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Marocco, Legge 09-08 sulla protezione dei dati e disciplina DGSSI; cooperazione con l'Europa significativa, ma trasferimenti da strutturare con garanzie. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Marocco, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,4/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,4	4,7	5,6	5,1	7,6	6,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,9	5,5	5,7	6,1	5,7	5,4

Il GCRI di Marocco è 6,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,1/10), mentre il più basso è Trasferibilità dati (5,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Marocco, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Marocco, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Marocco, Dal punto di vista italiano, Marocco rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Marocco è indicata una cooperazione selettiva, coerente con il FOTR di 5,7/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasferibilità dati a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

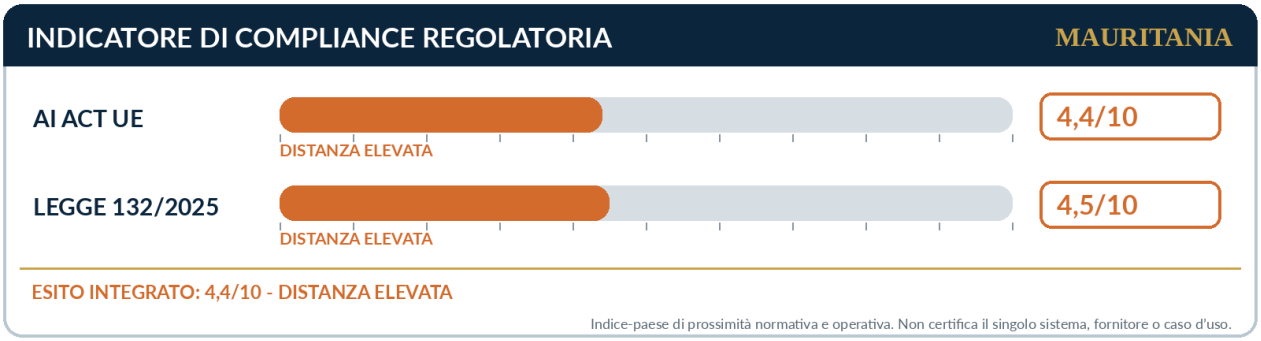
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Marocco: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Mauritania

Posizione FOTR	150	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,5	GCRI / 10	3,7	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Mauritania, AI Act UE 4,4/10; legge 132/2025 4,5/10; esito integrato 4,4/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Mauritania, situato in Africa occidentale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 38/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (3,7/10) e indice FOTR (4,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Mauritania è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	45,8% / 0,9 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	52,2% / 52 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	34,9 / 37,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	39,3/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	28,9/100 - rank 138	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (38/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	1,5 / 3,2 / 4,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Mauritania, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Mauritania le evidenze principali sono GTMI 37,4/100, EGDI 34,9/100, GCI 39,3/100, AI readiness 28,9/100. La dimensione più robusta è indipendenza della supply chain (4,5/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Mauritania è 4,2/10. La base statistica rileva utenti Internet pari al 45,8% nel 2024; 0,9 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 52,2% nel 2024; 52 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Mauritania al posto 138 con un valore medio di 28,9/100; il pilastro migliore è governance (40,5/100), quello più debole è sviluppo e diffusione (16,0/100). Il GTMI 2025 è 37,4/100. Il punteggio S2 è 2,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Mauritania è valutata fragile, con S3 pari a 3,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 29,6/100, sviluppo e diffusione dell'IA 16,0/100, penetrazione Internet 45,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Mauritania ottiene S4 4,5/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Mauritania, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre

ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,5/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Mauritania è S5 4,1/10. La base ITU registra ITU GCI 39,3/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è sviluppo delle capacità (1,1/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (38/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	1,5	Crimini finanziari	6,5
Reti criminali	5,5	Attori incorporati nello Stato	6,5
Attori stranieri	5,0	Attori del settore privato	3,5
Resilienza complessiva	3,2	Cooperazione internazionale	4,0
Politiche e norme nazionali	3,5	Forze dell'ordine	3,0
Antiriciclaggio	4,5	Prevenzione	2,5
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	4,8 - MODERATO

Sintesi del rischio cybercrime. Mauritania presenta un'esposizione stimata moderata (4,8/10): reati cyber-dipendenti 1,5/10, crimini finanziari 6,5/10 e resilienza 3,2/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (6,5/10) e reti criminali (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Mauritania assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Mauritania, la resilienza complessiva è molto debole (3,2/10); la cooperazione internazionale è debole (4,0/10), le politiche e norme nazionali sono deboli (3,5/10) e la capacità delle forze dell'ordine è molto debole (3,0/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 2,5/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Mauritania, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Mauritania. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Mauritania, In Mauritania le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Mauritania, Il livello governativo di Mauritania presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Mauritania, Sul piano militare e dual-use, Mauritania mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Mauritania, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Mauritania, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,1/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
4,2	2,9	3,0	4,5	4,1	3,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,7	4,6	4,3	5,0	4,5	4,1

Il GCRI di Mauritania è 3,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,0/10), mentre il più basso è Trasferibilità dati (4,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Mauritania, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Mauritania, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Mauritania, Dal punto di vista italiano, Mauritania rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Mauritania ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

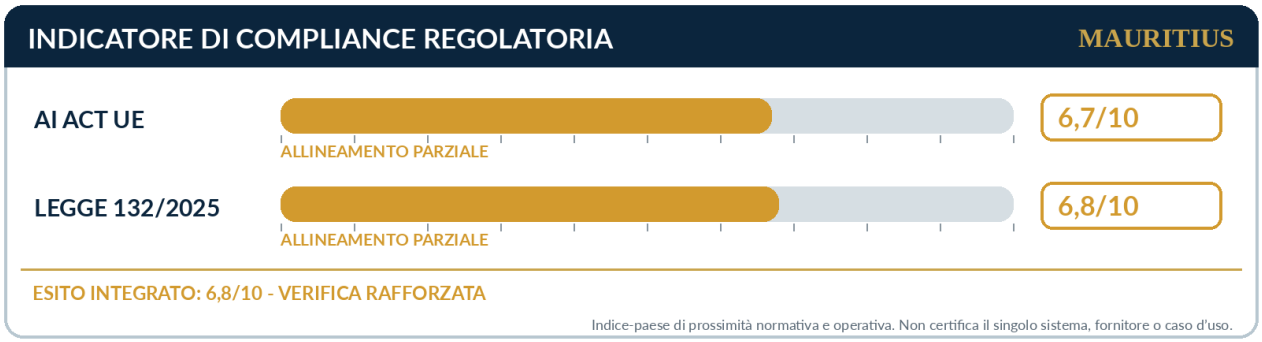
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Mauritania: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Mauritius

Posizione FOTR	53	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	6,8	GCRI / 10	7,0	Classe operativa	Affidabilità favorevole ma condizionata

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Mauritius, AI Act UE 6,7/10; legge 132/2025 6,8/10; esito integrato 6,8/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Mauritius non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 87/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,0/10) e indice FOTR (6,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Mauritius dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	73,3% / 28,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 2.158 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	75,1 / 94,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	100,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	54,6/100 - rank 67	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (87/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,0 / 5,6 / 4,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Mauritius, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Mauritius le evidenze principali sono GTMI 94,4/100, EGDI 75,1/100, GCI 100,0/100, AI readiness 54,6/100. La dimensione più robusta è postura di sicurezza cyber (8,8/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,3/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Mauritius è 8,1/10. La base statistica rileva utenti Internet pari al 73,3% nel 2024; 28,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 2.158 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Mauritius al posto 67 con un valore medio di 54,6/100; il pilastro migliore è governance (72,5/100), quello più debole è resilienza (36,8/100). Il GTMI 2025 è 94,4/100. Il punteggio S2 è 6,2/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Mauritius è valutata sufficiente ma disomogenea, con S3 pari a 6,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 74,6/100, sviluppo e diffusione dell'IA 38,5/100, penetrazione Internet 73,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Mauritius ottiene S4 5,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Mauritius, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=5,3/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Mauritius è S5 8,8/10. La base ITU registra ITU GCI 100,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure giuridiche (20,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (87/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Data Protection Act 2017, Computer Misuse and Cybercrime Act e convergenza con standard internazionali; ecosistema favorevole ai servizi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,0	Crimini finanziari	5,5
Reti criminali	5,5	Attori incorporati nello Stato	5,0
Attori stranieri	4,0	Attori del settore privato	5,0
Resilienza complessiva	5,6	Cooperazione internazionale	6,5
Politiche e norme nazionali	6,0	Forze dell'ordine	5,5
Antiriciclaggio	4,0	Prevenzione	5,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	4,6 - MODERATO

Quadro criminale digitale. Per Mauritius, l'indice operativo FOTR-CY è 4,6/10, classe moderata. Il mercato dei reati cyber-dipendenti è intermedio (4,0/10), mentre i crimini finanziari sono elevati (5,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (5,5/10) e attori incorporati nello Stato (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Mauritius assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Mauritius, la resilienza complessiva è intermedia (5,6/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 5,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Mauritius, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Mauritius. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Mauritius, In Mauritius le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Mauritius, Il livello governativo di Mauritius presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Mauritius, Sul piano militare e dual-use, Mauritius mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Mauritius, Data Protection Act 2017, Computer Misuse and Cybercrime Act e convergenza con standard internazionali; ecosistema favorevole ai servizi. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Mauritius, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 6,6/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,1	6,2	6,5	5,3	8,8	7,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
7,0	6,6	6,9	7,1	6,2	6,6

Il GCRI di Mauritius è 7,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (7,1/10), mentre il più basso è Supply chain (6,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Mauritius, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Mauritius, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Mauritius, Dal punto di vista italiano, Mauritius rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Mauritius è favorevole ma condizionata: il valore FOTR di 6,8/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Supply chain.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

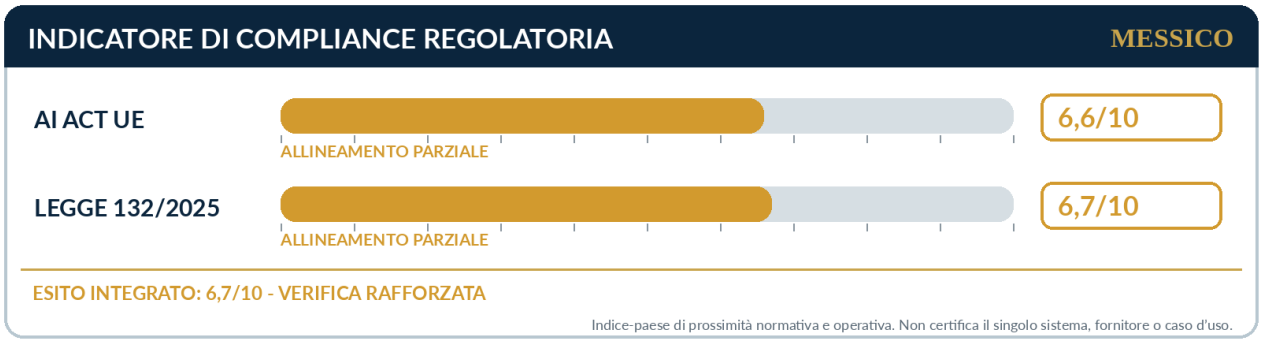
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Mauritius: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Messico

Posizione FOTR	54	Area	Americhe	Subregione	America centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	6,7	GCRI / 10	6,6	Classe operativa	Affidabilità favorevole ma condizionata

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Messico, AI Act UE 6,6/10; legge 132/2025 6,7/10; esito integrato 6,7/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Messico è stato membro delle nazioni unite collocato in America centrale. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 58/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,6/10) e indice FOTR (6,7/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. In Messico la trasformazione digitale procede più rapidamente dell'uniformità regolatoria e operativa. Gli investimenti devono essere accompagnati da audit, clausole di uscita e gestione locale del rischio.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	83,1% / 21,7 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	99,8% / 532 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	78,5 / 82,5	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	85,8/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	47,9/100 - rank 77	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	61/100 - Parzialmente libero / Parzialmente libero (58/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Firmatario/invitato	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	8,0 / 4,5 / 7,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Messico, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Messico le evidenze principali sono GTMI 82,5/100, EGDI 78,5/100, GCI 85,8/100, AI readiness 47,9/100. La dimensione più robusta è maturità infrastrutturale (7,7/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,8/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Messico è 7,7/10. La base statistica rileva utenti Internet pari al 83,1% nel 2024; 21,7 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 99,8% nel 2024; 532 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Messico al posto 77 con un valore medio di 47,9/100; il pilastro migliore è governance (67,6/100), quello più debole è resilienza (32,2/100). Il GTMI 2025 è 82,5/100. Il punteggio S2 è 5,9/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Messico è valutata sufficiente ma disomogenea, con S3 pari a 6,3/10. Le evidenze disponibili comprendono indice UN di capitale umano 76,0/100, sviluppo e diffusione dell'IA 34,1/100, penetrazione Internet 83,1%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Messico ottiene S4 5,8/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Messico, Forte integrazione con gli Stati Uniti, accompagnata da fornitori europei e asiatici e da capacità locali. L'impatto sulla valutazione è misurato da S4=5,8/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Messico è S5 7,5/10. La base ITU registra ITU GCI 85,8/100, Tier 2 - avanzato; il pilastro relativamente più debole è cooperazione (13,4/20). Freedom on the Net è 61/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (58/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Firmatario/invitato. Quadro normativo sintetico: LFPDPPP per il settore privato, legge generale per soggetti pubblici e normativa cyber frammentata; trasferimenti UE normalmente basati su garanzie contrattuali.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	8,0	Crimini finanziari	8,5
Reti criminali	8,5	Attori incorporati nello Stato	7,5
Attori stranieri	4,0	Attori del settore privato	6,5
Resilienza complessiva	4,5	Cooperazione internazionale	7,0
Politiche e norme nazionali	5,5	Forze dell'ordine	5,0
Antiriciclaggio	4,5	Prevenzione	4,0
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	7,1 - ALTO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (8,0/10), criminalità finanziaria (8,5/10) e resilienza (4,5/10) colloca Messico in una fascia di rischio alto, pari a 7,1/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (8,5/10) e attori incorporati nello Stato (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Messico assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Messico, la resilienza complessiva è debole (4,5/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 4,0/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Messico, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Messico. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Messico, In Messico le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Messico, Il livello governativo di Messico presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Messico, Sul piano militare e dual-use, Messico mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Messico, LFPDPPP per il settore privato, legge generale per soggetti pubblici e normativa cyber frammentata; trasferimenti UE normalmente basati su garanzie contrattuali. Lo stato rispetto alla Convenzione di Budapest è: Firmatario/invitato; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Messico, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 6,3/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,7	5,9	6,3	5,8	7,5	6,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,9	6,5	6,6	7,2	6,7	6,3

Il GCRI di Messico è 6,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (7,2/10), mentre il più basso è Trasferibilità dati (6,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Messico, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Messico, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Messico, Dal punto di vista italiano, Messico rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Messico è favorevole ma condizionata: il valore FOTR di 6,7/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Trasferibilità dati.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

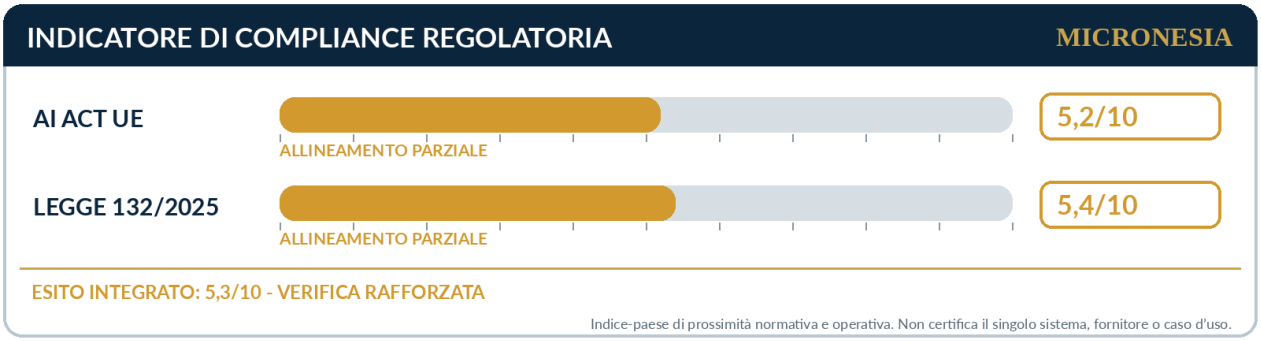
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Messico: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Micronesia

Posizione FOTR	109	Area	Oceania	Subregione	Pacifico insulare
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Media	Copertura dati	5/7 famiglie
FOTR / 10	5,6	GCRI / 10	3,4	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Micronesia, AI Act UE 5,2/10; legge 132/2025 5,4/10; esito integrato 5,3/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Oceania, Micronesia presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La distanza geografica e l'insularità rendono centrali cavi sottomarini, satelliti, continuità energetica e dipendenza da fornitori australiani, neozelandesi, statunitensi o asiatici. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 92/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,6/10) supera il GCRI tecnico (3,4/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. In Micronesia la trasformazione digitale procede più rapidamente dell'uniformità regolatoria e operativa. Gli investimenti devono essere accompagnati da audit, clausole di uscita e gestione locale del rischio.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	39,5% / 5,8 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	88,9% / 194 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	32,4 / 8,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	8,8/100 - Tier 5 - capacità iniziali	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	n.d./100 - rank n.d.	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (92/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	1,5 / 5,5 / 3,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Micronesia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 5/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Micronesia le evidenze principali sono GTMI 8,6/100, EGDI 32,4/100, GCI 8,8/100. La dimensione più robusta è capitale umano e competenze digitali (5,8/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (1,5/10). Sono disponibili 5 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata media. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Micronesia è 3,3/10. La base statistica rileva utenti Internet pari al 39,5% nel 2024; 5,8 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 88,9% nel 2024; 194 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Per Micronesia non è disponibile un profilo Oxford Insights direttamente attribuibile; l'adozione di IA è quindi valutata attraverso GovTech, servizi online, infrastrutture e fonti qualitative. Il GTMI 2025 è 8,6/100. Il punteggio S2 è 1,5/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Micronesia è valutata sufficiente ma disomogenea, con S3 pari a 5,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 57,3/100, penetrazione Internet 39,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Micronesia ottiene S4 3,9/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Micronesia, Dipendenza da Australia, Nuova Zelanda, Stati Uniti, Francia e operatori satellitari o sottomarini; la scala ridotta limita la diversificazione e aumenta il rischio di concentrazione. L'impatto sulla

valutazione è misurato da S4=3,9/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Micronesia è S5 2,5/10. La base ITU registra ITU GCI 8,8/100, Tier 5 - capacità iniziali; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (92/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	1,5	Crimini finanziari	2,5
Reti criminali	4,5	Attori incorporati nello Stato	3,0
Attori stranieri	4,5	Attori del settore privato	1,5
Resilienza complessiva	5,5	Cooperazione internazionale	6,5
Politiche e norme nazionali	6,0	Forze dell'ordine	6,5
Antiriciclaggio	5,0	Prevenzione	5,0
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	3,1 - MODERATO

Quadro criminale digitale. Per Micronesia, l'indice operativo FOTR-CY è 3,1/10, classe moderata. Il mercato dei reati cyber-dipendenti è limitato o poco osservabile (1,5/10), mentre i crimini finanziari sono limitati o poco osservabili (2,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (4,5/10) e attori stranieri (4,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Micronesia assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Micronesia, la resilienza complessiva è intermedia (5,5/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è intermedia (6,5/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 5,0/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Micronesia, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Micronesia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Micronesia, In Micronesia le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Micronesia, Il livello governativo di Micronesia presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Micronesia, Sul piano militare e dual-use, Micronesia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Micronesia, Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Micronesia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,5/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,3	1,5	5,8	3,9	2,5	3,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,6	4,8	6,2	6,4	4,6	5,5

Il GCRI di Micronesia è 3,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,4/10), mentre il più basso è Supply chain (4,6/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio-alto	Medio	Medio	Medio

La matrice applica il FOTR di 5,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Micronesia, 1 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Cloud e infrastrutture. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Micronesia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Micronesia, Dal punto di vista italiano, Micronesia rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Micronesia è indicata una cooperazione selettiva, coerente con il FOTR di 5,6/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Cloud e infrastrutture a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

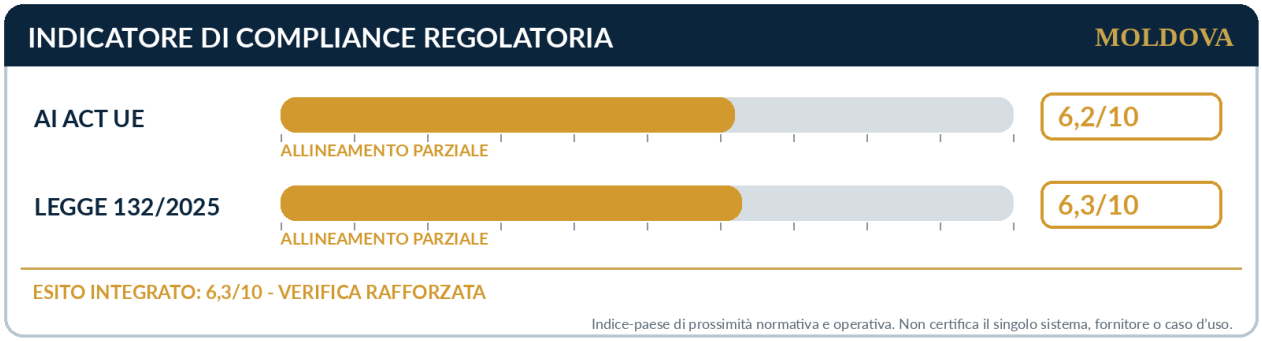
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Micronesia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Media con copertura 5/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Moldova

Posizione FOTR	67	Area	Europa	Subregione	Europa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	6,2	GCRI / 10	6,5	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Moldova, AI Act UE 6,2/10; legge 132/2025 6,3/10; esito integrato 6,3/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Moldova, situato in Europa orientale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La prossimità europea può ridurre i costi operativi, ma non sostituisce la verifica dell'allineamento al GDPR, delle autorità indipendenti e della reale origine dei servizi cloud. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Cina, Russia, Turchia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 60/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,5/10) e indice FOTR (6,2/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il quadro di Moldova è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	77,4% / 29,6 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 13.318 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	77,2 / 85,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	65,1/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	55,3/100 - rank 71	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (60/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,5 / 4,1 / 6,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Moldova, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Moldova le evidenze principali sono GTMI 85,4/100, EGDI 77,2/100, GCI 65,1/100, AI readiness 55,3/100. La dimensione più robusta è maturità infrastrutturale (8,1/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (5,8/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Moldova è 8,1/10. La base statistica rileva utenti Internet pari al 77,4% nel 2024; 29,6 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 13.318 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Moldova al posto 71 con un valore medio di 55,3/100; il pilastro migliore è adozione pubblica (82,3/100), quello più debole è sviluppo e diffusione (22,4/100). Il GTMI 2025 è 85,4/100. Il punteggio S2 è 6,3/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Moldova è valutata sufficiente ma disomogenea, con S3 pari a 5,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 77,8/100, sviluppo e diffusione dell'IA 22,4/100, penetrazione Internet 77,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Moldova ottiene S4 6,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Cina, Russia, Turchia; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Moldova, Mercato multi-fornitore tra Unione europea, Stati Uniti, Turchia, Cina e, in alcuni segmenti, Russia; il peso relativo varia tra pubblico, telecomunicazioni e difesa. L'impatto sulla valutazione è

misurato da S4=6,1/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Moldova è S5 6,3/10. La base ITU registra ITU GCI 65,1/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (6,7/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (60/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge sulla protezione dei dati e percorso di convergenza con l'acquis UE; capacità cyber in crescita, ma ancora disomogenea.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,5	Crimini finanziari	8,0
Reti criminali	5,0	Attori incorporati nello Stato	8,0
Attori stranieri	5,5	Attori del settore privato	7,0
Resilienza complessiva	4,1	Cooperazione internazionale	5,5
Politiche e norme nazionali	5,5	Forze dell'ordine	4,0
Antiriciclaggio	4,0	Prevenzione	3,5
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	6,8 - ALTO

Quadro criminale digitale. Per Moldova, l'indice operativo FOTR-CY è 6,8/10, classe alta. Il mercato dei reati cyber-dipendenti è molto elevato (7,5/10), mentre i crimini finanziari sono molto elevati (8,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e attori del settore privato (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Moldova assumono particolare rilevanza ransomware come servizio, malware sottrattori di informazioni, infrastrutture di hosting permissive, DDoS, furto di credenziali, estorsione dei dati e possibili sovrapposizioni tra criminalità professionale e finalità geopolitiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Moldova, la resilienza complessiva è debole (4,1/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 3,5/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Moldova, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; blocco di hosting e ASN ad alta reputazione negativa, ricerca proattiva delle minacce su malware sottrattori di informazioni e controllo dei canali RDP/VPN; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Moldova. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Moldova, In Moldova le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Moldova, Il livello governativo di Moldova presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Moldova, Sul piano militare e dual-use, Moldova mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Moldova, Legge sulla protezione dei dati e percorso di convergenza con l'acquis UE; capacità cyber in crescita, ma ancora disomogenea. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Moldova, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,9/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,1	6,3	5,8	6,1	6,3	6,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,7	6,0	5,8	7,1	5,7	5,9

Il GCRI di Moldova è 6,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (7,1/10), mentre il più basso è Supply chain (5,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Moldova, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Moldova, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Moldova, Dal punto di vista italiano, Moldova rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Moldova è indicata una cooperazione selettiva, coerente con il FOTR di 6,2/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Supply chain a decisione caso per caso.

Presidi minimi raccomandati

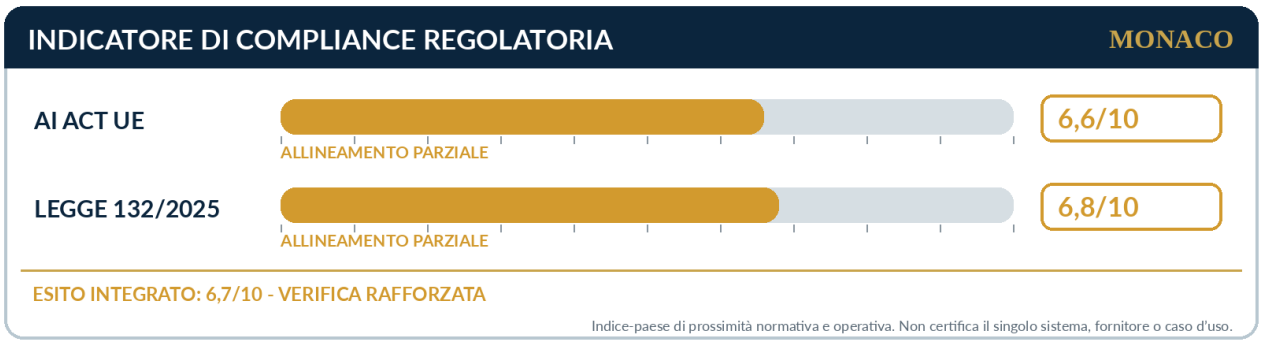
Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Moldova: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Monaco

Posizione FOTR	**51**	**Area**	Europa	**Subregione**	Europa occidentale e centrale
Status	**Stato membro delle Nazioni Unite**	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	**6,9**	**GCRI / 10**	**6,7**	**Classe operativa**	**Affidabilità favorevole ma condizionata**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Monaco, AI Act UE 6,6/10; legge 132/2025 6,8/10; esito integrato 6,7/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Monaco non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La prossimità europea può ridurre i costi operativi, ma non sostituisce la verifica dell'allineamento al GDPR, delle autorità indipendenti e della reale origine dei servizi cloud. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, Russia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 82/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,7/10) e indice FOTR (6,9/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il quadro di Monaco è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	99,0% / 55,7 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 41.495 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	71,7 / 36,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	75,4/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	37,2/100 - rank 105	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (82/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,5 / 5,8 / 3,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Monaco, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Monaco le evidenze principali sono GTMI 36,6/100, EGDI 71,7/100, GCI 75,4/100, AI readiness 37,2/100. La dimensione più robusta è maturità infrastrutturale (9,6/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,0/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Monaco è 9,6/10. La base statistica rileva utenti Internet pari al 99,0% nel 2024; 55,7 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 41.495 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Monaco al posto 105 con un valore medio di 37,2/100; il pilastro migliore è governance (57,4/100), quello più debole è politiche pubbliche (12,0/100). Il GTMI 2025 è 36,6/100. Il punteggio S2 è 4,0/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Monaco è valutata sufficiente ma disomogenea, con S3 pari a 6,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 75,1/100, sviluppo e diffusione dell'IA 35,0/100, penetrazione Internet 99,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Monaco ottiene S4 6,2/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, Russia; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Monaco, Ecosistema multi-fornitore con dipendenze europee, statunitensi, russe o cinesi da verificare per singolo settore e livello di governo. L'impatto sulla valutazione è misurato da S4=6,2/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Monaco è S5 7,3/10. La base ITU registra ITU GCI 75,4/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (13,7/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (82/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Disciplina nazionale della protezione dei dati, delle comunicazioni elettroniche e dei reati informatici, con differenze rispetto al GDPR; trasferimenti e accessi pubblici richiedono una verifica locale aggiornata.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,5	Crimini finanziari	3,5
Reti criminali	2,5	Attori incorporati nello Stato	3,5
Attori stranieri	5,5	Attori del settore privato	5,0
Resilienza complessiva	5,8	Cooperazione internazionale	5,5
Politiche e norme nazionali	7,0	Forze dell'ordine	7,0
Antiriciclaggio	5,0	Prevenzione	5,5
Supporto vittime e testimoni	8,0	Rischio operativo FOTR-CY	3,5 - MODERATO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (2,5/10), criminalità finanziaria (3,5/10) e resilienza (5,8/10) colloca Monaco in una fascia di rischio moderato, pari a 3,5/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (5,5/10) e attori del settore privato (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Monaco assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Monaco, la resilienza complessiva è intermedia (5,8/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è intermedia (7,0/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 5,5/10 e supporto a vittime e testimoni 8,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Monaco, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Monaco. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Monaco, In Monaco le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Monaco, Il livello governativo di Monaco presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Monaco, Sul piano militare e dual-use, Monaco mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Monaco, Disciplina nazionale della protezione dei dati, delle comunicazioni elettroniche e dei reati informatici, con differenze rispetto al GDPR; trasferimenti e accessi pubblici richiedono una verifica locale aggiornata. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Monaco, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 6,5/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,6	4,0	6,2	6,2	7,3	6,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
7,1	7,1	6,8	6,9	6,7	6,5

Il GCRI di Monaco è 6,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,9/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (7,1/10), mentre il più basso è Trasferibilità dati (6,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,9/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Monaco, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Monaco, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Monaco, Dal punto di vista italiano, Monaco rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Monaco è favorevole ma condizionata: il valore FOTR di 6,9/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Trasferibilità dati.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

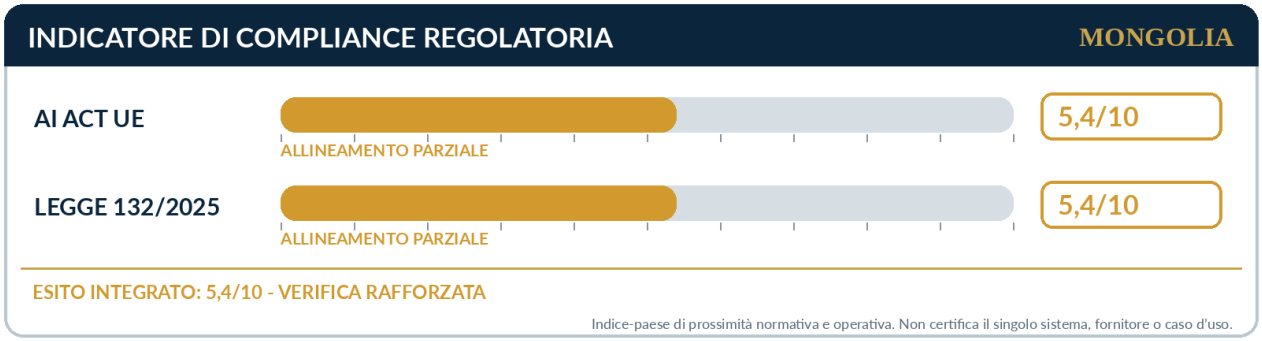
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Monaco: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Mongolia

Posizione FOTR	122	Area	Asia	Subregione	Asia orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,4	GCRI / 10	6,0	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Mongolia, AI Act UE 5,4/10; legge 132/2025 5,4/10; esito integrato 5,4/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Mongolia è stato membro delle nazioni unite collocato in Asia orientale. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 84/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,0/10) e indice FOTR (5,4/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Mongolia è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	85,1% / 15,8 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	99,1% / 2.564 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	84,6 / 77,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	56,4/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	42,0/100 - rank 94	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (84/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,0 / 5,3 / 5,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Mongolia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Mongolia le evidenze principali sono GTMI 77,6/100, EGDI 84,6/100, GCI 56,4/100, AI readiness 42,0/100. La dimensione più robusta è maturità infrastrutturale (7,9/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,3/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Mongolia è 7,9/10. La base statistica rileva utenti Internet pari al 85,1% nel 2024; 15,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 99,1% nel 2024; 2.564 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Mongolia al posto 94 con un valore medio di 42,0/100; il pilastro migliore è adozione pubblica (69,4/100), quello più debole è sviluppo e diffusione (20,5/100). Il GTMI 2025 è 77,6/100. Il punteggio S2 è 5,4/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Mongolia è valutata sufficiente ma disomogenea, con S3 pari a 5,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 77,7/100, sviluppo e diffusione dell'IA 20,5/100, penetrazione Internet 85,1%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Mongolia ottiene S4 5,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Mongolia, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo

societario e subfornitura. L'impatto sulla valutazione è misurato da S4=5,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Mongolia è S5 5,6/10. La base ITU registra ITU GCI 56,4/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è cooperazione (6,5/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (84/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,0	Crimini finanziari	5,0
Reti criminali	4,5	Attori incorporati nello Stato	5,5
Attori stranieri	5,0	Attori del settore privato	5,0
Resilienza complessiva	5,3	Cooperazione internazionale	6,5
Politiche e norme nazionali	6,5	Forze dell'ordine	5,0
Antiriciclaggio	5,0	Prevenzione	6,0
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	5,2 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Mongolia il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,2/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 6,0/10; le frodi e i reati finanziari 5,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (5,5/10) e attori stranieri (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Mongolia assumono particolare rilevanza compromissioni della supply chain, sottrazione di proprietà intellettuale, furto di cripto-attività, phishing mirato, abuso di identità digitali e intrusioni persistenti contro industria e amministrazioni. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Mongolia, la resilienza complessiva è debole (5,3/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 6,0/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Mongolia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Mongolia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Mongolia, In Mongolia le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La superficie di

rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Mongolia, Il livello governativo di Mongolia presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Mongolia, Sul piano militare e dual-use, Mongolia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Mongolia, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Mongolia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,9/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,9	5,4	5,6	5,3	5,6	6,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,6	5,8	5,0	5,4	5,3	4,9

Il GCRI di Mongolia è 6,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (5,8/10), mentre il più basso è Trasferibilità dati (4,9/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 5,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Mongolia, 5 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Mongolia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Mongolia, Dal punto di vista italiano, Mongolia rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Mongolia è indicata una cooperazione selettiva, coerente con il FOTR di 5,4/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

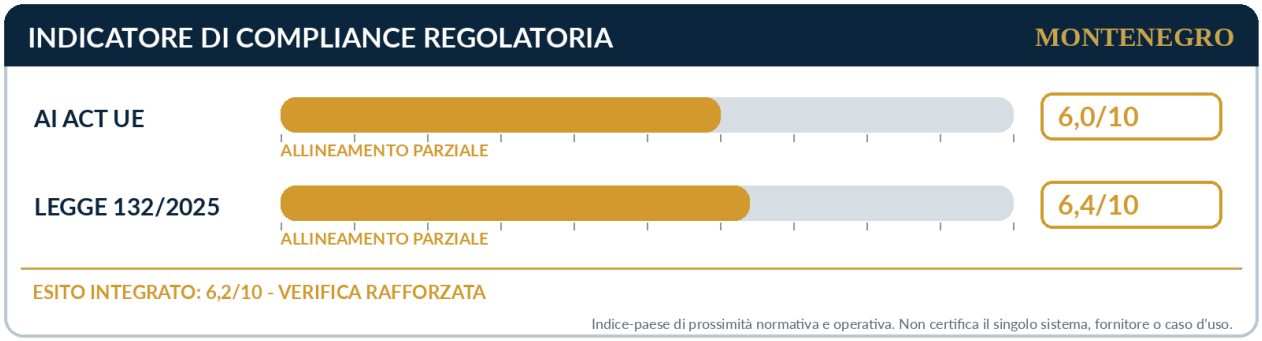
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Mongolia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Montenegro

Posizione FOTR	62	Area	Europa	Subregione	Europa sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	6,3	GCRI / 10	6,3	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Montenegro, AI Act UE 6,0/10; legge 132/2025 6,4/10; esito integrato 6,2/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Europa, Montenegro presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La collocazione nell'Alleanza Atlantica favorisce interoperabilità e cooperazione di sicurezza, senza equivalere automaticamente ad allineamento pieno sul diritto dei dati. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Cina, Russia, Turchia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 68/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,3/10) e indice FOTR (6,3/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Montenegro dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	88,9% / 32,3 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 6.425 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	72,1 / 51,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	74,8/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	40,9/100 - rank 100	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (68/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 4,8 / 5,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Montenegro, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Montenegro le evidenze principali sono GTMI 51,3/100, EGDI 72,1/100, GCI 74,8/100, AI readiness 40,9/100. La dimensione più robusta è maturità infrastrutturale (8,8/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,4/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Montenegro è 8,8/10. La base statistica rileva utenti Internet pari al 88,9% nel 2024; 32,3 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 6.425 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Montenegro al posto 100 con un valore medio di 40,9/100; il pilastro migliore è governance (53,8/100), quello più debole è sviluppo e diffusione (26,9/100). Il GTMI 2025 è 51,3/100. Il punteggio S2 è 4,4/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Montenegro è valutata sufficiente ma disomogenea, con S3 pari a 5,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 71,9/100, sviluppo e diffusione dell'IA 26,9/100, penetrazione Internet 88,9%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Montenegro ottiene S4 5,9/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Cina, Russia, Turchia; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Montenegro, Mercato multi-fornitore tra Unione europea, Stati Uniti, Turchia, Cina e, in alcuni segmenti, Russia; il peso relativo varia tra pubblico, telecomunicazioni e difesa. L'impatto sulla valutazione è

misurato da S4=5,9/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Montenegro è S5 6,9/10. La base ITU registra ITU GCI 74,8/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (5,3/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (68/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Quadro nazionale di protezione dati e cybersicurezza in progressivo allineamento all'acquis dell'Unione europea; la distanza tra legge formale, vigilanza e prassi deve essere verificata nel settore interessato.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	6,0
Reti criminali	7,0	Attori incorporati nello Stato	7,0
Attori stranieri	6,0	Attori del settore privato	5,0
Resilienza complessiva	4,8	Cooperazione internazionale	6,5
Politiche e norme nazionali	5,0	Forze dell'ordine	4,5
Antiriciclaggio	5,0	Prevenzione	5,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	5,7 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Montenegro presenta un'esposizione stimata significativa (5,7/10): reati cyber-dipendenti 5,0/10, crimini finanziari 6,0/10 e resilienza 4,8/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (7,0/10) e attori incorporati nello Stato (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Montenegro assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Montenegro, la resilienza complessiva è debole (4,8/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 5,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Montenegro, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Montenegro. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Montenegro, In Montenegro le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Montenegro, Il livello governativo di Montenegro presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Montenegro, Sul piano militare e dual-use, Montenegro mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Montenegro, Quadro nazionale di protezione dati e cybersicurezza in progressivo allineamento all'acquis dell'Unione europea; la distanza tra legge formale, vigilanza e prassi deve essere verificata nel settore interessato. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Montenegro, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,5/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,8	4,4	5,6	5,9	6,9	6,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,3	6,1	5,7	8,3	5,8	5,5

Il GCRI di Montenegro è 6,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,3/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (8,3/10), mentre il più basso è Trasferibilità dati (5,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,3/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Montenegro, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Montenegro, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Montenegro, Dal punto di vista italiano, Montenegro rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Montenegro è indicata una cooperazione selettiva, coerente con il FOTR di 6,3/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasferibilità dati a decisione caso per caso.

Presidi minimi raccomandati

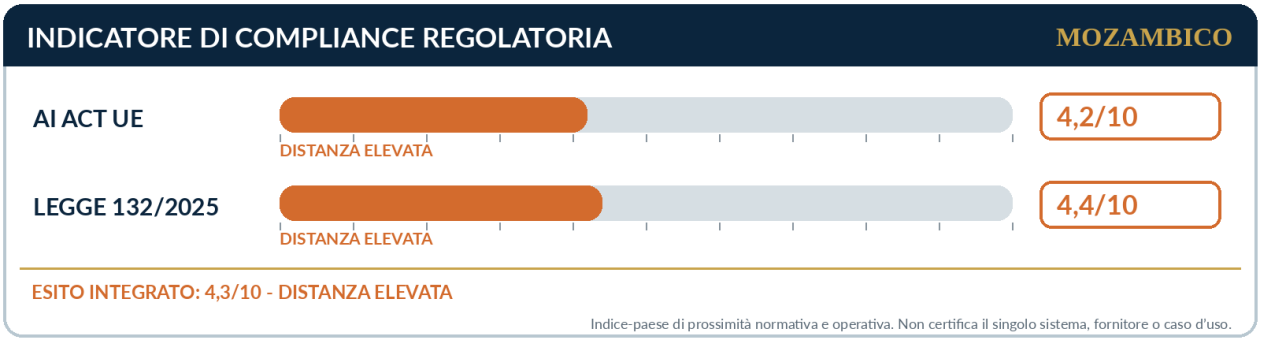
Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Montenegro: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Mozambico

Posizione FOTR	168	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,4	GCRI / 10	3,6	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Mozambico, AI Act UE 4,2/10; legge 132/2025 4,4/10; esito integrato 4,3/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Mozambico, situato in Africa orientale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 42/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (3,6/10) e indice FOTR (4,4/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per Mozambico non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	20,5% / 0,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	36,9% / 37 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	28,5 / 39,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	66,0/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	22,7/100 - rank 161	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (42/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Firmatario/invitato	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,5 / 3,2 / 6,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Mozambico, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Mozambico le evidenze principali sono GTMI 39,3/100, EGDI 28,5/100, GCI 66,0/100, AI readiness 22,7/100. La dimensione più robusta è postura di sicurezza cyber (5,8/10), mentre la criticità relativa riguarda maturità infrastrutturale (1,5/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Mozambico è 1,5/10. La base statistica rileva utenti Internet pari al 20,5% nel 2024; 0,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 36,9% nel 2024; 37 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Mozambico al posto 161 con un valore medio di 22,7/100; il pilastro migliore è resilienza (35,4/100), quello più debole è politiche pubbliche (8,0/100). Il GTMI 2025 è 39,3/100. Il punteggio S2 è 2,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Mozambico è valutata fragile, con S3 pari a 3,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 39,5/100, sviluppo e diffusione dell'IA 11,5/100, penetrazione Internet 20,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Mozambico ottiene S4 4,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Mozambico, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre

ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,6/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Mozambico è S5 5,8/10. La base ITU registra ITU GCI 66,0/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (7,9/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (42/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Firmatario/invitato. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,5	Crimini finanziari	7,0
Reti criminali	8,0	Attori incorporati nello Stato	9,0
Attori stranieri	7,5	Attori del settore privato	4,0
Resilienza complessiva	3,2	Cooperazione internazionale	5,5
Politiche e norme nazionali	5,5	Forze dell'ordine	2,0
Antiriciclaggio	3,0	Prevenzione	3,0
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	6,2 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Mozambico presenta un'esposizione stimata significativa (6,2/10): reati cyber-dipendenti 3,5/10, crimini finanziari 7,0/10 e resilienza 3,2/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e reti criminali (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Mozambico assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Mozambico, la resilienza complessiva è molto debole (3,2/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è molto debole (2,0/10). Completano il quadro antiriciclaggio 3,0/10, prevenzione 3,0/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Mozambico, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Mozambico. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Mozambico, In Mozambico le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i

partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Mozambico, Il livello governativo di Mozambico presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Mozambico, Sul piano militare e dual-use, Mozambico mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Mozambico, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Firmatario/invitato; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Mozambico, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,0/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
1,5	2,9	3,2	4,6	5,8	3,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,3	4,2	4,5	5,0	4,1	4,0

Il GCRI di Mozambico è 3,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,0/10), mentre il più basso è Trasferibilità dati (4,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Mozambico, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Mozambico, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Mozambico, Dal punto di vista italiano, Mozambico rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Mozambico ricade nella fascia di alto rischio (4,4/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

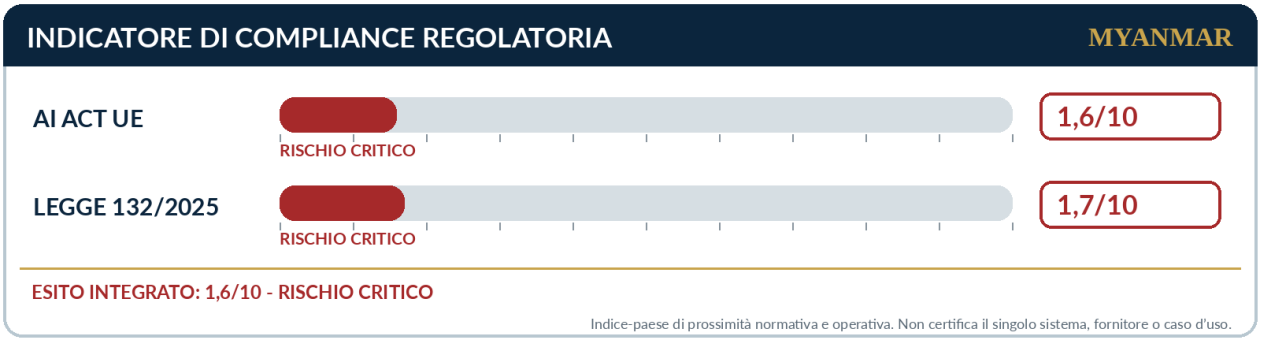
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Mozambico: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Myanmar

Posizione FOTR	194	Area	Asia	Subregione	Asia sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	1,5	GCRI / 10	3,4	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Myanmar, AI Act UE 1,6/10; legge 132/2025 1,7/10; esito integrato 1,6/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Per un operatore italiano, Myanmar non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 4/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (3,4/10) è superiore al punteggio FOTR (1,5/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Il rapporto digitale con Myanmar deve essere considerato eccezionale e ad alta esposizione. Sono necessari screening sanzionatori, autorizzazioni, segregazione completa e impossibilità tecnica di accedere ai dati in chiaro.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	45,4% / 2,9 per 100	2020/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	80,4% / 24 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	50,0 / 46,1	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	73,7/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	19,1/100 - rank 173	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	9/100 - Non libero / Non libero (4/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,5 / 1,5 / 8,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Myanmar, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Myanmar le evidenze principali sono GTMI 46,1/100, EGDI 50,0/100, GCI 73,7/100, AI readiness 19,1/100. La dimensione più robusta è maturità infrastrutturale (4,3/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,8/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Myanmar è 4,3/10. La base statistica rileva utenti Internet pari al 45,4% nel 2020; 2,9 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 80,4% nel 2024; 24 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Myanmar al posto 173 con un valore medio di 19,1/100; il pilastro migliore è infrastrutture IA (33,2/100), quello più debole è politiche pubbliche (8,0/100). Il GTMI 2025 è 46,1/100. Il punteggio S2 è 2,8/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Myanmar è valutata fragile, con S3 pari a 3,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 50,8/100, sviluppo e diffusione dell'IA 18,6/100, penetrazione Internet 45,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Myanmar ottiene S4 3,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Myanmar, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo

societario e subfornitura. L'impatto sulla valutazione è misurato da S4=3,6/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Myanmar è S5 3,5/10. La base ITU registra ITU GCI 73,7/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (10,9/20). Freedom on the Net è 9/100 - Non libero, mentre Freedom in the World è Non libero (4/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Electronic Transactions Law, Cybersecurity Law e poteri estesi in un contesto politico instabile; accessi pubblici e continuità presentano criticità elevate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,5	Crimini finanziari	8,5
Reti criminali	8,0	Attori incorporati nello Stato	9,0
Attori stranieri	9,0	Attori del settore privato	7,5
Resilienza complessiva	1,5	Cooperazione internazionale	2,0
Politiche e norme nazionali	2,0	Forze dell'ordine	1,5
Antiriciclaggio	1,5	Prevenzione	1,0
Supporto vittime e testimoni	1,0	Rischio operativo FOTR-CY	8,5 - CRITICO

Quadro criminale digitale. Per Myanmar, l'indice operativo FOTR-CY è 8,5/10, classe critica. Il mercato dei reati cyber-dipendenti è molto elevato (7,5/10), mentre i crimini finanziari sono molto elevati (8,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e attori stranieri (9,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Myanmar assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Myanmar, la resilienza complessiva è molto debole (1,5/10); la cooperazione internazionale è molto debole (2,0/10), le politiche e norme nazionali sono molto deboli (2,0/10) e la capacità delle forze dell'ordine è molto debole (1,5/10). Completano il quadro antiriciclaggio 1,5/10, prevenzione 1,0/10 e supporto a vittime e testimoni 1,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Myanmar, il livello critico non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; controllo della filiera contro esposizione a complessi organizzati per truffe telematiche, call center coercitivi e conti prestanome; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Myanmar. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Myanmar, In Myanmar le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. Per

i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Myanmar, Il livello governativo di Myanmar presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Myanmar, Sul piano militare e dual-use, Myanmar mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Myanmar, Electronic Transactions Law, Cybersecurity Law e poteri estesi in un contesto politico instabile; accessi pubblici e continuità presentano criticità elevate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Myanmar, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 0,0/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
4,3	2,8	3,0	3,6	3,5	3,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
2,1	2,4	0,0	2,3	2,5	0,0

Il GCRI di Myanmar è 3,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 1,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Supply chain (2,5/10), mentre il più basso è Trasparenza istituzionale (0,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 1,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Myanmar, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Myanmar, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Myanmar, Dal punto di vista italiano, Myanmar rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Myanmar, il FOTR di 1,5/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

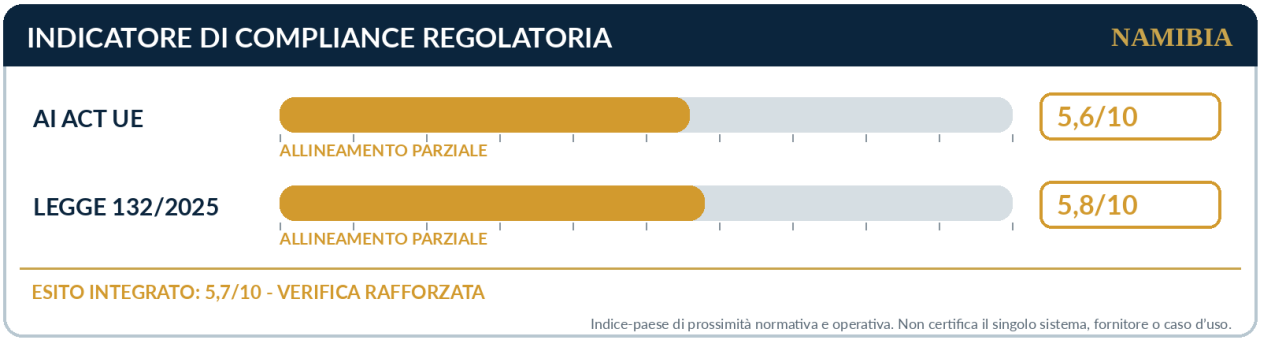
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Myanmar: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Namibia

Posizione FOTR	89	Area	Africa	Subregione	Africa australe
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,8	GCRI / 10	4,7	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Namibia, AI Act UE 5,6/10; legge 132/2025 5,8/10; esito integrato 5,7/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Namibia è stato membro delle nazioni unite collocato in Africa australe. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 73/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,8/10) supera il GCRI tecnico (4,7/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il quadro di Namibia è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	64,9% / 2,8 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	59,3% / 427 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	60,1 / 36,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	36,9/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	37,9/100 - rank 110	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (73/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 4,6 / 5,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Namibia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Namibia le evidenze principali sono GTMI 36,3/100, EGDI 60,1/100, GCI 36,9/100, AI readiness 37,9/100. La dimensione più robusta è maturità infrastrutturale (5,5/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Namibia è 5,5/10. La base statistica rileva utenti Internet pari al 64,9% nel 2024; 2,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 59,3% nel 2024; 427 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Namibia al posto 110 con un valore medio di 37,9/100; il pilastro migliore è governance (52,9/100), quello più debole è politiche pubbliche (19,5/100). Il GTMI 2025 è 36,3/100. Il punteggio S2 è 3,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Namibia è valutata sufficiente ma disomogenea, con S3 pari a 5,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 57,4/100, sviluppo e diffusione dell'IA 28,2/100, penetrazione Internet 64,9%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Namibia ottiene S4 4,8/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Namibia, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,8/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Namibia è S5 4,4/10. La base ITU registra ITU GCI 36,9/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (3,5/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (73/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber in sviluppo, con tutele costituzionali e regole settoriali; assenza di un regime maturo richiede garanzie contrattuali robuste.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	5,0
Reti criminali	5,5	Attori incorporati nello Stato	6,0
Attori stranieri	6,5	Attori del settore privato	4,5
Resilienza complessiva	4,6	Cooperazione internazionale	6,5
Politiche e norme nazionali	6,5	Forze dell'ordine	3,5
Antiriciclaggio	3,5	Prevenzione	4,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	5,6 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Namibia presenta un'esposizione stimata significativa (5,6/10): reati cyber-dipendenti 5,5/10, crimini finanziari 5,0/10 e resilienza 4,6/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (6,5/10) e attori incorporati nello Stato (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Namibia assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Namibia, la resilienza complessiva è debole (4,6/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è debole (3,5/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 4,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Namibia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Namibia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Namibia, In Namibia le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Namibia, Il livello governativo di Namibia presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Namibia, Sul piano militare e dual-use, Namibia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Namibia, Quadro privacy e cyber in sviluppo, con tutele costituzionali e regole settoriali; assenza di un regime maturo richiede garanzie contrattuali robuste. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Namibia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,4/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
5,5	3,9	5,0	4,8	4,4	4,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,7	5,7	5,9	6,5	5,6	5,4

Il GCRI di Namibia è 4,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,5/10), mentre il più basso è Trasferibilità dati (5,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Namibia, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Namibia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Namibia, Dal punto di vista italiano, Namibia rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Namibia è indicata una cooperazione selettiva, coerente con il FOTR di 5,8/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasferibilità dati a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

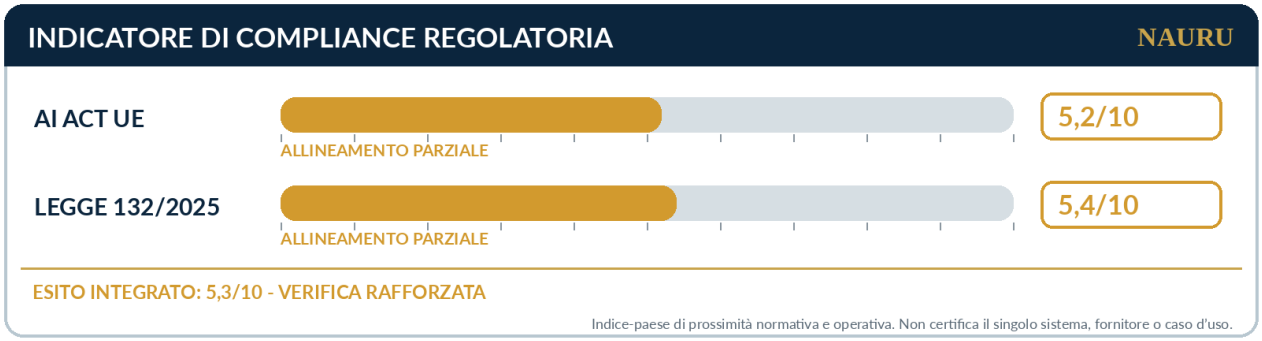
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Namibia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Nauru

Posizione FOTR	115	Area	Oceania	Subregione	Pacifico insulare
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,5	GCRI / 10	3,9	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Nauru, AI Act UE 5,2/10; legge 132/2025 5,4/10; esito integrato 5,3/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Oceania, Nauru presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La distanza geografica e l'insularità rendono centrali cavi sottomarini, satelliti, continuità energetica e dipendenza da fornitori australiani, neozelandesi, statunitensi o asiatici. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 75/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,5/10) supera il GCRI tecnico (3,9/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il quadro di Nauru è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	83,0% / 10,0 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 670 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	44,5 / 13,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	21,6/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	19,6/100 - rank 160	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (75/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	1,0 / 4,8 / 2,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Nauru, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Nauru le evidenze principali sono GTMI 13,8/100, EGDI 44,5/100, GCI 21,6/100, AI readiness 19,6/100. La dimensione più robusta è maturità infrastrutturale (6,3/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Nauru è 6,3/10. La base statistica rileva utenti Internet pari al 83,0% nel 2024; 10,0 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 100,0% nel 2024; 670 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Nauru al posto 160 con un valore medio di 19,6/100; il pilastro migliore è infrastrutture IA (41,7/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 13,8/100. Il punteggio S2 è 2,1/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Nauru è valutata fragile, con S3 pari a 3,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 50,6/100, sviluppo e diffusione dell'IA 21,0/100, penetrazione Internet 83,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Nauru ottiene S4 4,0/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Nauru, Dipendenza da Australia, Nuova Zelanda, Stati Uniti, Francia e operatori satellitari o sottomarini; la scala ridotta limita la diversificazione e aumenta il rischio di concentrazione. L'impatto sulla

valutazione è misurato da S4=4,0/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Nauru è S5 3,2/10. La base ITU registra ITU GCI 21,6/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (75/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	1,0	Crimini finanziari	2,5
Reti criminali	1,5	Attori incorporati nello Stato	3,5
Attori stranieri	2,0	Attori del settore privato	1,5
Resilienza complessiva	4,8	Cooperazione internazionale	6,0
Politiche e norme nazionali	7,0	Forze dell'ordine	5,0
Antiriciclaggio	7,0	Prevenzione	1,0
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	2,7 - CONTENUTO

Quadro criminale digitale. Per Nauru, l'indice operativo FOTR-CY è 2,7/10, classe contenuta. Il mercato dei reati cyber-dipendenti è limitato o poco osservabile (1,0/10), mentre i crimini finanziari sono limitati o poco osservabili (2,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (3,5/10) e attori stranieri (2,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Nauru assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Nauru, la resilienza complessiva è debole (4,8/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 7,0/10, prevenzione 1,0/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Nauru, il livello contenuto non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Nauru. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Nauru, In Nauru le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Nauru, Il livello governativo di Nauru presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve

essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Nauru, Sul piano militare e dual-use, Nauru mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Nauru, Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Nauru, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,4/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,3	2,1	3,8	4,0	3,2	3,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,8	4,8	5,7	6,5	4,5	5,4

Il GCRI di Nauru è 3,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,5/10), mentre il più basso è Supply chain (4,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio-alto	Medio-alto	Medio-alto	Medio

La matrice applica il FOTR di 5,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Nauru, 3 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Cloud e infrastrutture, IP e R&S, Pubblica amministrazione. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Nauru, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Nauru, Dal punto di vista italiano, Nauru rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Nauru è indicata una cooperazione selettiva, coerente con il FOTR di 5,5/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Cloud e infrastrutture a decisione caso per caso.

Presidi minimi raccomandati

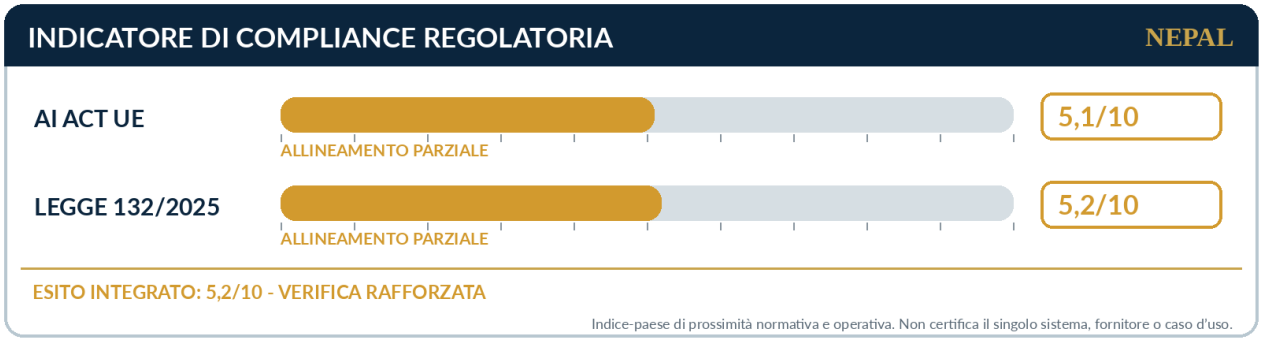
Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Nauru: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Nepal

Posizione FOTR	128	Area	Asia	Subregione	Asia meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,2	GCRI / 10	5,3	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Nepal, AI Act UE 5,1/10; legge 132/2025 5,2/10; esito integrato 5,2/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Nepal, situato in Asia meridionale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 59/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,3/10) e indice FOTR (5,2/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Nepal è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	46,3% / 10,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	97,9% / 541 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	57,8 / 51,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	69,8/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	41,5/100 - rank 106	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (59/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,0 / 3,9 / 6,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Nepal, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Nepal le evidenze principali sono GTMI 51,7/100, EGDI 57,8/100, GCI 69,8/100, AI readiness 41,5/100. La dimensione più robusta è postura di sicurezza cyber (6,4/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,4/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Nepal è 6,0/10. La base statistica rileva utenti Internet pari al 46,3% nel 2024; 10,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 97,9% nel 2024; 541 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Nepal al posto 106 con un valore medio di 41,5/100; il pilastro migliore è governance (57,2/100), quello più debole è sviluppo e diffusione (22,5/100). Il GTMI 2025 è 51,7/100. Il punteggio S2 è 4,4/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Nepal è valutata fragile, con S3 pari a 4,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 52,1/100, sviluppo e diffusione dell'IA 22,5/100, penetrazione Internet 46,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Nepal ottiene S4 5,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Nepal, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo societario e

subfornitura. L'impatto sulla valutazione è misurato da S4=5,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Nepal è S5 6,4/10. La base ITU registra ITU GCI 69,8/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è cooperazione (9,4/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (59/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,0	Crimini finanziari	7,0
Reti criminali	7,5	Attori incorporati nello Stato	8,0
Attori stranieri	7,5	Attori del settore privato	7,5
Resilienza complessiva	3,9	Cooperazione internazionale	5,5
Politiche e norme nazionali	4,5	Forze dell'ordine	4,5
Antiriciclaggio	3,5	Prevenzione	3,5
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	6,1 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (4,0/10), criminalità finanziaria (7,0/10) e resilienza (3,9/10) colloca Nepal in una fascia di rischio significativo, pari a 6,1/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e reti criminali (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Nepal assumono particolare rilevanza compromissione delle caselle di posta aziendale, frodi da call center, abuso di portafogli digitali mobili, identità sintetiche, ransomware, phishing bancario e triangolazioni transfrontaliere dei proventi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Nepal, la resilienza complessiva è debole (3,9/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono deboli (4,5/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 3,5/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Nepal, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Nepal. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Nepal, In Nepal le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Nepal, Il livello governativo di Nepal presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Nepal, Sul piano militare e dual-use, Nepal mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Nepal, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Nepal, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,9/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,0	4,4	4,5	5,1	6,4	5,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,3	5,7	4,8	5,1	5,6	4,9

Il GCRI di Nepal è 5,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Maturità cyber (5,7/10), mentre il più basso è Trasparenza istituzionale (4,8/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 5,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Nepal, 5 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Nepal, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Nepal, Dal punto di vista italiano, Nepal rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Nepal è indicata una cooperazione selettiva, coerente con il FOTR di 5,2/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.
Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

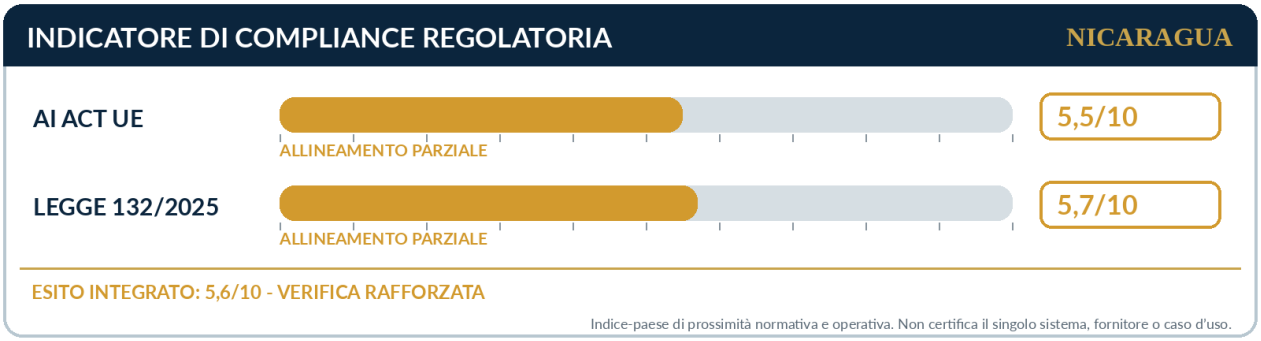
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Nepal: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Nicaragua

Posizione FOTR	90	Area	Americhe	Subregione	America centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,8	GCRI / 10	4,1	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Nicaragua, AI Act UE 5,5/10; legge 132/2025 5,7/10; esito integrato 5,6/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Nicaragua non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 14/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,8/10) supera il GCRI tecnico (4,1/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Nicaragua dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	61,4% / 5,8 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	88,7% / 94 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	53,2 / n.d.	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	20,6/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	21,7/100 - rank 163	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	38/100 - Non libero / Non libero (14/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,5 / 2,0 / 5,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Nicaragua, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Nicaragua le evidenze principali sono EGDI 53,2/100, GCI 20,6/100, AI readiness 21,7/100. La dimensione più robusta è maturità infrastrutturale (5,3/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,6/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Nicaragua è 5,3/10. La base statistica rileva utenti Internet pari al 61,4% nel 2024; 5,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 88,7% nel 2024; 94 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Nicaragua al posto 163 con un valore medio di 21,7/100; il pilastro migliore è governance (41,7/100), quello più debole è politiche pubbliche (7,5/100). Il punteggio S2 è 2,6/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Nicaragua è valutata fragile, con S3 pari a 4,3/10. Le evidenze disponibili comprendono indice UN di capitale umano 56,1/100, sviluppo e diffusione dell'IA 11,9/100, penetrazione Internet 61,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Nicaragua ottiene S4 4,9/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Nicaragua, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=4,9/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Nicaragua è S5 3,5/10. La base ITU registra ITU GCI 20,6/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è 38/100 - Non libero, mentre Freedom in the World è Non libero (14/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,5	Crimini finanziari	4,0
Reti criminali	6,5	Attori incorporati nello Stato	9,0
Attori stranieri	7,0	Attori del settore privato	4,5
Resilienza complessiva	2,0	Cooperazione internazionale	2,0
Politiche e norme nazionali	3,0	Forze dell'ordine	2,0
Antiriciclaggio	2,5	Prevenzione	3,0
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	5,9 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Nicaragua il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,9/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 3,5/10; le frodi e i reati finanziari 4,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e attori stranieri (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Nicaragua assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Nicaragua, la resilienza complessiva è molto debole (2,0/10); la cooperazione internazionale è molto debole (2,0/10), le politiche e norme nazionali sono molto deboli (3,0/10) e la capacità delle forze dell'ordine è molto debole (2,0/10). Completano il quadro antiriciclaggio 2,5/10, prevenzione 3,0/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Nicaragua, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Nicaragua. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Nicaragua, In Nicaragua le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Nicaragua, Il livello governativo di Nicaragua presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Nicaragua, Sul piano militare e dual-use, Nicaragua mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Nicaragua, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Nicaragua, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,8/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
5,3	2,6	4,3	4,9	3,5	4,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,0	5,8	5,5	6,0	5,5	5,8

Il GCRI di Nicaragua è 4,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (6,0/10), mentre il più basso è Trasparenza istituzionale (5,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Nicaragua, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Nicaragua, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Nicaragua, Dal punto di vista italiano, Nicaragua rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Nicaragua è indicata una cooperazione selettiva, coerente con il FOTR di 5,8/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasparenza istituzionale a decisione caso per caso.

Presidi minimi raccomandati

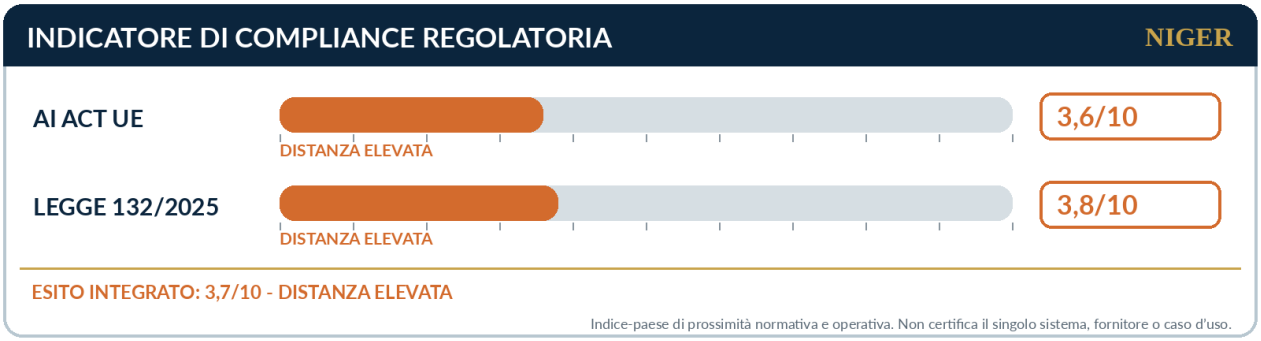
Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Nicaragua: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Niger

Posizione FOTR	181	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	3,8	GCRI / 10	2,3	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Niger, AI Act UE 3,6/10; legge 132/2025 3,8/10; esito integrato 3,7/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Niger è stato membro delle nazioni unite collocato in Africa occidentale. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 27/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (3,8/10) supera il GCRI tecnico (2,3/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. In Niger la cooperazione tecnologica ordinaria deve essere limitata a progetti non critici, con isolamento, cifratura e supervisione italiana. Investimenti strategici necessitano di autorizzazioni e valutazioni rafforzate.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	15,6% / 0,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	21,3% / 5 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	21,2 / 14,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	41,9/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	17,6/100 - rank 184	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (27/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	1,0 / 3,0 / 5,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Niger, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Niger le evidenze principali sono GTMI 14,7/100, EGDI 21,2/100, GCI 41,9/100, AI readiness 17,6/100. La dimensione più robusta è indipendenza della supply chain (3,4/10), mentre la criticità relativa riguarda maturità infrastrutturale (0,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Niger è 0,9/10. La base statistica rileva utenti Internet pari al 15,6% nel 2024; 0,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 21,3% nel 2024; 5 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Niger al posto 184 con un valore medio di 17,6/100; il pilastro migliore è governance (38,9/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 14,7/100. Il punteggio S2 è 1,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Niger è valutata fragile, con S3 pari a 2,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 16,9/100, sviluppo e diffusione dell'IA 9,2/100, penetrazione Internet 15,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Niger ottiene S4 3,4/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Niger, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=3,4/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Niger è S5 3,1/10. La base ITU registra ITU GCI 41,9/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (1,4/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (27/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	1,0	Crimini finanziari	6,5
Reti criminali	7,0	Attori incorporati nello Stato	8,0
Attori stranieri	6,5	Attori del settore privato	3,0
Resilienza complessiva	3,0	Cooperazione internazionale	3,5
Politiche e norme nazionali	4,5	Forze dell'ordine	3,5
Antiriciclaggio	4,0	Prevenzione	2,5
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	5,4 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Niger restituisce un rischio FOTR-CY di 5,4/10 (significativo). La componente cyber-dipendente vale 1,0/10 e quella finanziaria 6,5/10; la risposta sistemica è valutata molto debole, con resilienza media di 3,0/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e reti criminali (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Niger assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Niger, la resilienza complessiva è molto debole (3,0/10); la cooperazione internazionale è debole (3,5/10), le politiche e norme nazionali sono deboli (4,5/10) e la capacità delle forze dell'ordine è debole (3,5/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 2,5/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Niger, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Niger. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Niger, In Niger le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Niger, Il livello governativo di Niger presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Niger, Sul piano militare e dual-use, Niger mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Niger, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Niger, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 2,9/10 e il rischio sui dati personali è Alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
0,9	1,9	2,1	3,4	3,1	2,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,6	3,2	3,4	4,9	3,4	2,9

Il GCRI di Niger è 2,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 3,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (4,9/10), mentre il più basso è Trasferibilità dati (2,9/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Alto	Alto	Alto	Alto	Alto	Medio-alto

La matrice applica il FOTR di 3,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Niger, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Niger, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Niger, Dal punto di vista italiano, Niger rientra nella classe «Rischio alto»: cooperazione eccezionale e ad alto controllo, subordinata a assenza di dati sensibili, verifica sanzionatoria, autorizzazioni interne e impossibilità di accesso ai sistemi strategici. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Niger ricade nella fascia di alto rischio (3,8/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

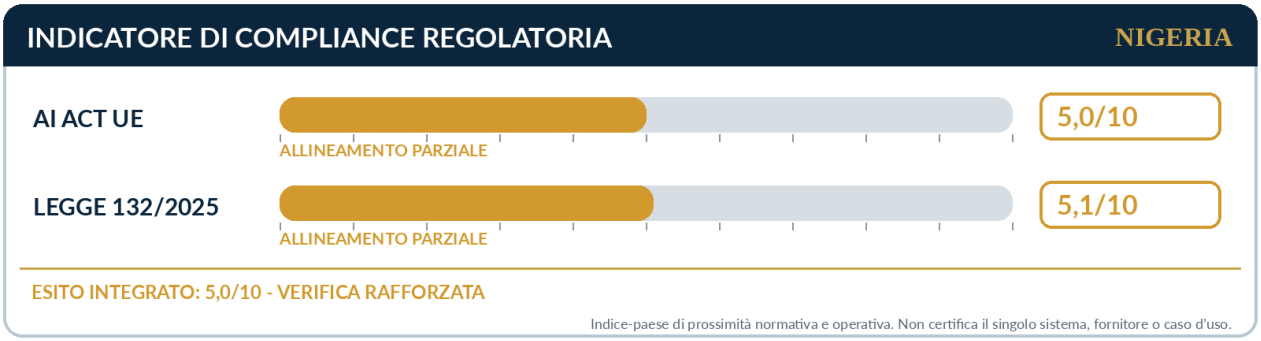
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Niger: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Nigeria

Posizione FOTR	135	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,0	GCRI / 10	5,3	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Nigeria, AI Act UE 5,0/10; legge 132/2025 5,1/10; esito integrato 5,0/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Nigeria presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 44/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,3/10) e indice FOTR (5,0/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Nigeria presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	41,2% / 0,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	62,5% / 98 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	48,1 / 51,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	82,4/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	54,5/100 - rank 70	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	59/100 - Parzialmente libero / Parzialmente libero (44/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,5 / 5,5 / 6,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Nigeria, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Nigeria le evidenze principali sono GTMI 51,2/100, EGDI 48,1/100, GCI 82,4/100, AI readiness 54,5/100. La dimensione più robusta è postura di sicurezza cyber (6,8/10), mentre la criticità relativa riguarda maturità infrastrutturale (3,9/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Nigeria è 3,9/10. La base statistica rileva utenti Internet pari al 41,2% nel 2024; 0,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 62,5% nel 2024; 98 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Nigeria al posto 70 con un valore medio di 54,5/100; il pilastro migliore è politiche pubbliche (80,5/100), quello più debole è infrastrutture IA (39,1/100). Il GTMI 2025 è 51,2/100. Il punteggio S2 è 5,2/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Nigeria è valutata fragile, con S3 pari a 4,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 42,4/100, sviluppo e diffusione dell'IA 39,5/100, penetrazione Internet 41,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Nigeria ottiene S4 5,6/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Nigeria, Mercato multi-fornitore con rilevante presenza cinese, statunitense, europea e capacità software locale. L'impatto sulla valutazione è misurato da S4=5,6/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Nigeria è S5 6,8/10. La base ITU registra ITU GCI 82,4/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (13,2/20). Freedom on the Net è 59/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (44/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Nigeria Data Protection Act 2023 e Cybercrimes Act; mercato digitale dinamico, ma enforcement, frodi e continuità restano disomogenei.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,5	Crimini finanziari	8,0
Reti criminali	8,0	Attori incorporati nello Stato	8,0
Attori stranieri	7,0	Attori del settore privato	7,0
Resilienza complessiva	5,5	Cooperazione internazionale	7,5
Politiche e norme nazionali	7,0	Forze dell'ordine	5,5
Antiriciclaggio	4,5	Prevenzione	5,5
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	6,6 - ALTO

Sintesi del rischio cybercrime. Nigeria presenta un'esposizione stimata alta (6,6/10): reati cyber-dipendenti 6,5/10, crimini finanziari 8,0/10 e resilienza 5,5/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (8,0/10) e attori incorporati nello Stato (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Nigeria assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Nigeria, la resilienza complessiva è debole (5,5/10); la cooperazione internazionale è robusta (7,5/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 5,5/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Nigeria, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Nigeria. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Nigeria, In Nigeria le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Nigeria, Il livello governativo di Nigeria presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Nigeria, Sul piano militare e dual-use, Nigeria mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Nigeria, Nigeria Data Protection Act 2023 e Cybercrimes Act; mercato digitale dinamico, ma enforcement, frodi e continuità restano disomogenei. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Nigeria, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,0/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,9	5,2	4,8	5,6	6,8	5,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,8	4,8	4,9	5,9	4,8	5,0

Il GCRI di Nigeria è 5,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,9/10), mentre il più basso è Compatibilità giuridica (4,8/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 5,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Nigeria, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Nigeria, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Nigeria, Dal punto di vista italiano, Nigeria rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Nigeria è indicata una cooperazione selettiva, coerente con il FOTR di 5,0/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

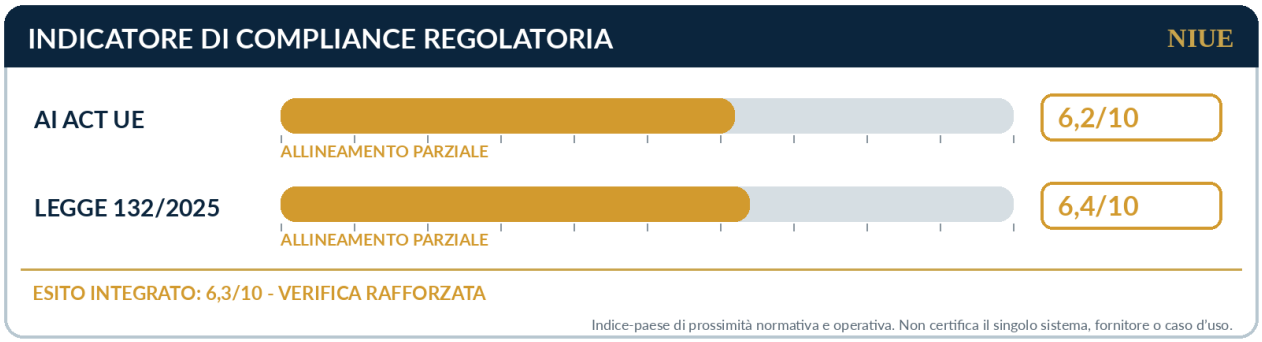
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Nigeria: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Niue

Posizione FOTR	63	Area	Oceania	Subregione	Pacifico insulare
Status	Stato autogovernato in libera associazione con la Nuova Zelanda	Confidenza Celeborn Intelligence	Bassa	Copertura dati	0/7 famiglie
FOTR / 10	6,3	GCRI / 10	5,8	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Niue, AI Act UE 6,2/10; legge 132/2025 6,4/10; esito integrato 6,3/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Niue, situato in Pacifico insulare, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La distanza geografica e l'insularità rendono centrali cavi sottomarini, satelliti, continuità energetica e dipendenza da fornitori australiani, neozelandesi, statunitensi o asiatici. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Per questa entità non è disponibile un indicatore Freedom in the World direttamente comparabile; l'assenza di copertura viene trattata come limite informativo e non come prova automatica di rischio. GCRI tecnico (5,8/10) e indice FOTR (6,3/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Niue dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	n.d. / n.d. per 100	n.d./n.d.	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	n.d. / n.d. per milione	n.d./n.d.	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	n.d. / n.d.	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	n.d./100 - n.d.	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	n.d./100 - rank n.d.	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / n.d.	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,3 / 7,5 / 5,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Niue, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 0/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Niue le evidenze principali sono nessun indicatore composito pienamente comparabile. La dimensione più robusta è capitale umano e competenze digitali (6,5/10), mentre la criticità relativa riguarda indipendenza della supply chain (4,6/10). Sono disponibili 0 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata bassa. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Niue è 5,8/10. La base statistica rileva i principali dati WDI non sono disponibili in forma omogenea. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Per Niue non è disponibile un profilo Oxford Insights direttamente attribuibile; l'adozione di IA è quindi valutata attraverso GovTech, servizi online, infrastrutture e fonti qualitative. Il punteggio S2 è 6,0/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Niue è valutata sufficiente ma disomogenea, con S3 pari a 6,5/10. Le evidenze disponibili comprendono evidenza quantitativa incompleta. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Niue ottiene S4 4,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Niue, Dipendenza da Australia, Nuova Zelanda, Stati Uniti, Francia e operatori satellitari o sottomarini; la scala ridotta limita la diversificazione e aumenta il rischio di concentrazione. L'impatto sulla valutazione è misurato da S4=4,6/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Niue è S5 5,9/10. La base ITU registra GCI non disponibile in forma comparabile. Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è n.d.. Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,3	Crimini finanziari	6,5
Reti criminali	5,8	Attori incorporati nello Stato	2,6
Attori stranieri	5,2	Attori del settore privato	4,5
Resilienza complessiva	7,5	Cooperazione internazionale	8,2
Politiche e norme nazionali	7,8	Forze dell'ordine	7,3
Antiriciclaggio	6,7	Prevenzione	7,0
Supporto vittime e testimoni	7,5	Rischio operativo FOTR-CY	5,0 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Niue presenta un'esposizione stimata significativa (5,0/10): reati cyber-dipendenti 6,3/10, crimini finanziari 6,5/10 e resilienza 7,5/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (5,8/10) e attori stranieri (5,2/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Niue assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Niue, la resilienza complessiva è intermedia (7,5/10); la cooperazione internazionale è robusta (8,2/10), le politiche e norme nazionali sono robuste (7,8/10) e la capacità delle forze dell'ordine è intermedia (7,3/10). Completano il quadro antiriciclaggio 6,7/10, prevenzione 7,0/10 e supporto a vittime e testimoni 7,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Niue, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori. Poiché l'entità non dispone di una serie nazionale GI-TOC autonoma, i valori derivano da un proxy Celeborn Intelligence ponderato su Nuova Zelanda 85%, Tonga 15%; la confidenza deve pertanto essere considerata inferiore e la decisione resa più prudente.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; proxy Celeborn Intelligence ponderato su Nuova Zelanda 85%, Tonga 15%. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Niue, In Niue le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Niue, Il livello governativo di Niue presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Niue, Sul piano militare e dual-use, Niue mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Niue, Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Niue, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 6,0/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
5,8	6,0	6,5	4,6	5,9	5,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,5	5,5	6,5	7,4	5,6	6,0

Il GCRI di Niue è 5,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,3/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (7,4/10), mentre il più basso è Maturità cyber (5,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,3/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Niue, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Niue, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Niue, Dal punto di vista italiano, Niue rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Niue è indicata una cooperazione selettiva, coerente con il FOTR di 6,3/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Maturità cyber a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

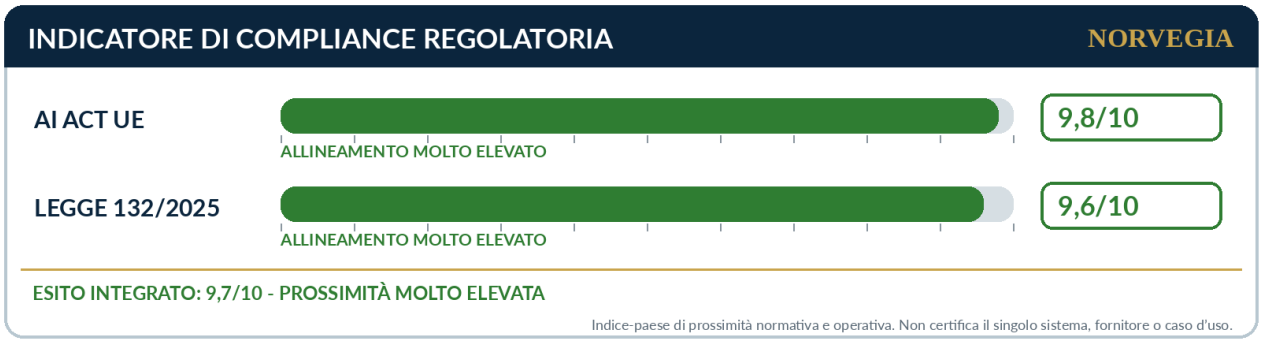
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Niue: World Development Indicators, valori più recenti disponibili 2022-2024; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Bassa con copertura 0/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Norvegia

Posizione FOTR	4	**Area**	Europa	**Subregione**	Europa settentrionale e baltica
Status	Stato membro delle Nazioni Unite	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	**9,3**	**GCRI / 10**	**8,5**	**Classe operativa**	**Affidabilità molto alta**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Norvegia, AI Act UE 9,8/10; legge 132/2025 9,6/10; esito integrato 9,7/10, classe «Allineamento molto elevato». L'integrazione nello Spazio economico europeo riduce la distanza regolatoria, senza eliminare la necessità di verificare autorità competenti, norme settoriali, trasferimenti e catena dei responsabili. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Per un operatore italiano, Norvegia non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La partecipazione allo Spazio economico europeo produce una forte prossimità normativa con l'Italia, pur richiedendo verifiche settoriali e contrattuali. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 99/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,5/10) e indice FOTR (9,3/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il sistema digitale di Norvegia è avanzato e integrato con standard internazionali. Le principali criticità non sono di base istituzionale, ma riguardano supply chain, concentrazione dei servizi e gestione delle eccezioni di sicurezza nazionale.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	99,0% / 45,2 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 35.470 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	93,2 / 77,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	97,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	78,3/100 - rank 10	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (99/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 7,9 / 4,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Norvegia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Norvegia le evidenze principali sono GTMI 77,9/100, EGDI 93,2/100, GCI 97,0/100, AI readiness 78,3/100. La dimensione più robusta è maturità infrastrutturale (9,8/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,6/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Norvegia è 9,8/10. La base statistica rileva utenti Internet pari al 99,0% nel 2024; 45,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 35.470 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Norvegia al posto 10 con un valore medio di 78,3/100; il pilastro migliore è governance (94,0/100), quello più debole è sviluppo e diffusione (60,6/100). Il GTMI 2025 è 77,9/100. Il punteggio S2 è 7,9/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Norvegia è valutata solida, con S3 pari a 8,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 91,7/100, sviluppo e diffusione dell'IA 60,6/100, penetrazione Internet 99,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Norvegia ottiene S4 6,6/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Norvegia, Fornitura prevalentemente nazionale, europea e statunitense, con catene hardware globali. In genere è possibile diversificare e imporre requisiti contrattuali elevati. L'impatto sulla valutazione è

misurato da S4=6,6/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Norvegia è S5 9,5/10. La base ITU registra ITU GCI 97,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è sviluppo delle capacità (17,7/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (99/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR attraverso lo SEE, Personal Data Act e Security Act; ampia convergenza con NIS2 e con gli standard europei.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	5,5
Reti criminali	5,0	Attori incorporati nello Stato	1,5
Attori stranieri	5,0	Attori del settore privato	2,0
Resilienza complessiva	7,9	Cooperazione internazionale	9,0
Politiche e norme nazionali	8,5	Forze dell'ordine	7,5
Antiriciclaggio	7,5	Prevenzione	7,5
Supporto vittime e testimoni	7,0	Rischio operativo FOTR-CY	4,1 - MODERATO

Sintesi del rischio cybercrime. Norvegia presenta un'esposizione stimata moderata (4,1/10): reati cyber-dipendenti 5,5/10, crimini finanziari 5,5/10 e resilienza 7,9/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (5,0/10) e attori stranieri (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Norvegia assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Norvegia, la resilienza complessiva è robusta (7,9/10); la cooperazione internazionale è robusta (9,0/10), le politiche e norme nazionali sono robuste (8,5/10) e la capacità delle forze dell'ordine è robusta (7,5/10). Completano il quadro antiriciclaggio 7,5/10, prevenzione 7,5/10 e supporto a vittime e testimoni 7,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Norvegia, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Norvegia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Norvegia, In Norvegia le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Norvegia, Il livello governativo di Norvegia presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Norvegia, Sul piano militare e dual-use, Norvegia mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Norvegia, GDPR attraverso lo SEE, Personal Data Act e Security Act; ampia convergenza con NIS2 e con gli standard europei. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Norvegia, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 10,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,8	7,9	8,5	6,6	9,5	8,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,7	9,1	9,2	9,1	8,7	10,0

Il GCRI di Norvegia è 8,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 9,3/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (10,0/10), mentre il più basso è Supply chain (8,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Basso	Basso	Basso

La matrice applica il FOTR di 9,3/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Norvegia, la matrice non individua ambiti ad alto rischio; 6 categorie risultano basse o medio-basse, ferma la verifica del singolo progetto. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Norvegia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Norvegia, Dal punto di vista italiano, Norvegia rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Norvegia, il FOTR di 9,3/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (8,7/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

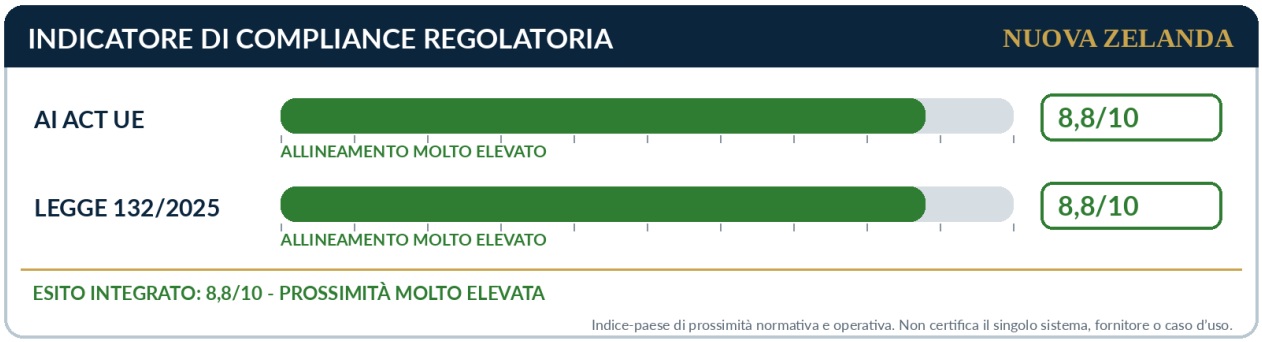
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Norvegia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Nuova Zelanda

Posizione FOTR	**13**	**Area**	Oceania	**Subregione**	Australia e Nuova Zelanda
Status	**Stato membro delle Nazioni Unite**	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	**9,0**	**GCRI / 10**	**7,7**	**Classe operativa**	**Affidabilità molto alta**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Nuova Zelanda, AI Act UE 8,8/10; legge 132/2025 8,8/10; esito integrato 8,8/10, classe «Allineamento molto elevato». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Nuova Zelanda è stato membro delle nazioni unite collocato in Australia e Nuova Zelanda. La partecipazione all'ecosistema Five Eyes rafforza l'integrazione informativa e tecnologica con il blocco anglosassone, ma rende necessario valutare i poteri di accesso extraterritoriale e la concentrazione cloud. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 99/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (9,0/10) supera il GCRI tecnico (7,7/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il sistema digitale di Nuova Zelanda è avanzato e integrato con standard internazionali. Le principali criticità non sono di base istituzionale, ma riguardano supply chain, concentrazione dei servizi e gestione delle eccezioni di sicurezza nazionale.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	93,5% / 38,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 18.709 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	92,7 / 87,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	82,6/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	66,5/100 - rank 37	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (99/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,0 / 7,9 / 5,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Nuova Zelanda, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Nuova Zelanda le evidenze principali sono GTMI 87,8/100, EGDI 92,7/100, GCI 82,6/100, AI readiness 66,5/100. La dimensione più robusta è maturità infrastrutturale (9,1/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Nuova Zelanda è 9,1/10. La base statistica rileva utenti Internet pari al 93,5% nel 2024; 38,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 18.709 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Nuova Zelanda al posto 37 con un valore medio di 66,5/100; il pilastro migliore è politiche pubbliche (92,0/100), quello più debole è sviluppo e diffusione (49,3/100). Il GTMI 2025 è 87,8/100. Il punteggio S2 è 7,3/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Nuova Zelanda è valutata sufficiente ma disomogenea, con S3 pari a 7,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 96,2/100, sviluppo e diffusione dell'IA 49,3/100, penetrazione Internet 93,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Nuova Zelanda ottiene S4 6,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Stati Uniti; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open

source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Nuova Zelanda, Prevalenza di fornitori australiani, statunitensi e britannici, con mercato locale di scala ridotta. L'impatto sulla valutazione è misurato da S4=6,1/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Nuova Zelanda è S5 8,4/10. La base ITU registra ITU GCI 82,6/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è cooperazione (14,3/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (99/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Privacy Act 2020, regime di notifica e supervisione; decisione UE di adeguatezza e stretta cooperazione con partner Five Eyes.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,0	Crimini finanziari	7,0
Reti criminali	6,0	Attori incorporati nello Stato	2,0
Attori stranieri	5,0	Attori del settore privato	5,0
Resilienza complessiva	7,9	Cooperazione internazionale	8,5
Politiche e norme nazionali	8,0	Forze dell'ordine	7,5
Antiriciclaggio	7,0	Prevenzione	7,5
Supporto vittime e testimoni	8,0	Rischio operativo FOTR-CY	5,0 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Nuova Zelanda restituisce un rischio FOTR-CY di 5,0/10 (significativo). La componente cyber-dipendente vale 7,0/10 e quella finanziaria 7,0/10; la risposta sistemica è valutata robusta, con resilienza media di 7,9/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (6,0/10) e attori stranieri (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Nuova Zelanda assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Nuova Zelanda, la resilienza complessiva è robusta (7,9/10); la cooperazione internazionale è robusta (8,5/10), le politiche e norme nazionali sono robuste (8,0/10) e la capacità delle forze dell'ordine è robusta (7,5/10). Completano il quadro antiriciclaggio 7,0/10, prevenzione 7,5/10 e supporto a vittime e testimoni 8,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Nuova Zelanda, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Nuova Zelanda. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Nuova Zelanda, In Nuova Zelanda le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Nuova Zelanda, Il livello governativo di Nuova Zelanda presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Nuova Zelanda, Sul piano militare e dual-use, Nuova Zelanda mostra stretta cooperazione con ecosistemi occidentali e capacità dual-use significative. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Nuova Zelanda, Privacy Act 2020, regime di notifica e supervisione; decisione UE di adeguatezza e stretta cooperazione con partner Five Eyes. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Nuova Zelanda, È disponibile una decisione UE di adeguatezza. L'operatore italiano deve comunque controllare la portata della decisione, i trasferimenti successivi, le misure di sicurezza e le eventuali discipline settoriali. La componente FOTR di trasferibilità è 10,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,1	7,3	7,8	6,1	8,4	7,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,1	9,3	7,5	9,4	8,7	10,0

Il GCRI di Nuova Zelanda è 7,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 9,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (10,0/10), mentre il più basso è Trasparenza istituzionale (7,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Medio-basso	Basso	Basso

La matrice applica il FOTR di 9,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Nuova Zelanda, la cautela si concentra su 1 ambiti a rischio intermedio: IP e R&S. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Nuova Zelanda, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Nuova Zelanda, Dal punto di vista italiano, Nuova Zelanda rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Nuova Zelanda, il FOTR di 9,0/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (7,5/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

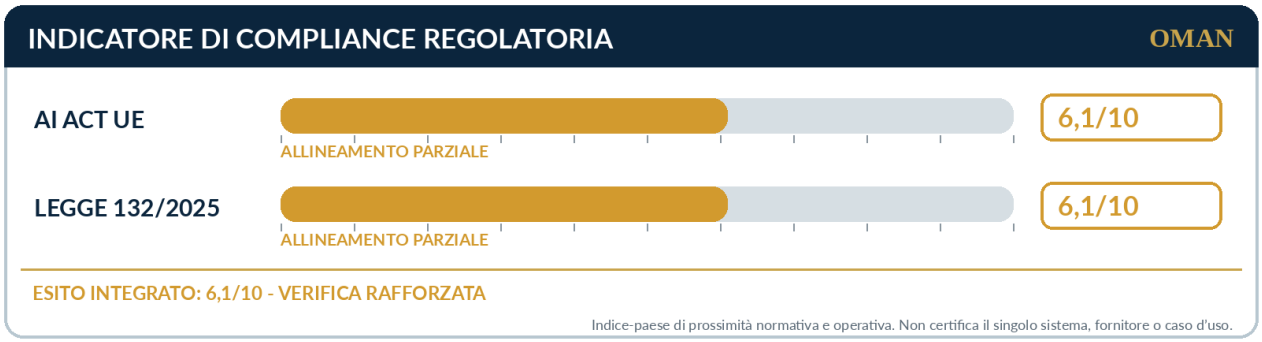
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Nuova Zelanda: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Oman

Posizione FOTR	**71**	**Area**	Asia	**Subregione**	Medio Oriente e Asia occidentale
Status	**Stato membro delle Nazioni Unite**	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	**6,1**	**GCRI / 10**	**7,0**	**Classe operativa**	**Affidabilità selettiva**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Oman, AI Act UE 6,1/10; legge 132/2025 6,1/10; esito integrato 6,1/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Asia, Oman presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 24/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,0/10) e indice FOTR (6,1/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. In Oman la trasformazione digitale procede più rapidamente dell'uniformità regolatoria e operativa. Gli investimenti devono essere accompagnati da audit, clausole di uscita e gestione locale del rischio.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	95,3% / 11,1 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 287 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	85,8 / 85,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	97,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	60,0/100 - rank 61	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (24/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 5,3 / 5,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Oman, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Oman le evidenze principali sono GTMI 85,4/100, EGDI 85,8/100, GCI 97,0/100, AI readiness 60,0/100. La dimensione più robusta è postura di sicurezza cyber (8,5/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,6/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Oman è 7,9/10. La base statistica rileva utenti Internet pari al 95,3% nel 2024; 11,1 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 287 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Oman al posto 61 con un valore medio di 60,0/100; il pilastro migliore è politiche pubbliche (88,5/100), quello più debole è sviluppo e diffusione (40,3/100). Il GTMI 2025 è 85,4/100. Il punteggio S2 è 6,6/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Oman è valutata sufficiente ma disomogenea, con S3 pari a 6,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 79,8/100, sviluppo e diffusione dell'IA 40,3/100, penetrazione Internet 95,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Oman ottiene S4 5,6/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Oman, Fornitori britannici, statunitensi, europei e asiatici, con crescente localizzazione. L'impatto sulla valutazione è misurato da S4=5,6/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Oman è S5 8,5/10. La base ITU registra ITU GCI 97,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure tecniche (18,4/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (24/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Personal Data Protection Law 6/2022 e disciplina settoriale; attuazione recente e requisiti di trasferimento da verificare.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	6,5
Reti criminali	5,0	Attori incorporati nello Stato	4,5
Attori stranieri	4,0	Attori del settore privato	5,5
Resilienza complessiva	5,3	Cooperazione internazionale	6,5
Politiche e norme nazionali	6,5	Forze dell'ordine	7,0
Antiriciclaggio	6,0	Prevenzione	5,0
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	5,0 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Oman restituisce un rischio FOTR-CY di 5,0/10 (significativo). La componente cyber-dipendente vale 5,0/10 e quella finanziaria 6,5/10; la risposta sistemica è valutata debole, con resilienza media di 5,3/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori del settore privato (5,5/10) e reti criminali (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Oman assumono particolare rilevanza phishing e credential theft, ransomware, frodi d'investimento, attacchi a energia e servizi pubblici, abuso di cripto-attività e campagne che possono combinare profitto, spionaggio e pressione politica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Oman, la resilienza complessiva è debole (5,3/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è intermedia (7,0/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 5,0/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Oman, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Oman. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Oman, In Oman le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Oman, Il livello governativo di Oman presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Oman, Sul piano militare e dual-use, Oman mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Oman, Personal Data Protection Law 6/2022 e disciplina settoriale; attuazione recente e requisiti di trasferimento da verificare. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Oman, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,8/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,9	6,6	6,6	5,6	8,5	7,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,1	6,5	5,8	6,3	6,0	5,8

Il GCRI di Oman è 7,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,1/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (6,5/10), mentre il più basso è Trasparenza istituzionale (5,8/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,1/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Oman, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Oman, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Oman, Dal punto di vista italiano, Oman rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Oman è indicata una cooperazione selettiva, coerente con il FOTR di 6,1/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasparenza istituzionale a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

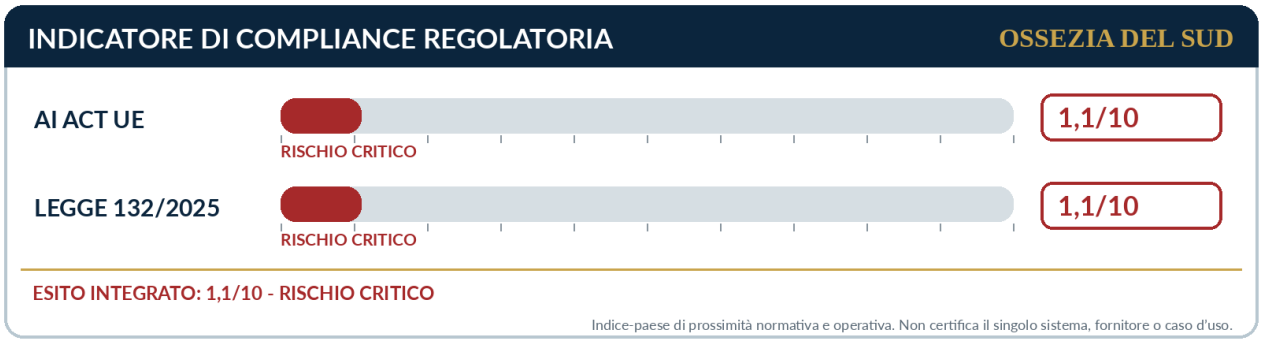
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Oman: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Ossezia del Sud

Posizione FOTR	203	Area	Asia	Subregione	Caucaso
Status	Entità de facto a riconoscimento limitato	Confidenza Celeborn Intelligence	Bassa	Copertura dati	0/7 famiglie
FOTR / 10	1,0	GCRI / 10	1,3	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Ossezia del Sud, AI Act UE 1,1/10; legge 132/2025 1,1/10; esito integrato 1,1/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Ossezia del Sud, situato in Caucaso, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Russia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 12/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (1,3/10) e indice FOTR (1,0/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Entità de facto con infrastrutture ridotte e dipendenza russa; cooperazione digitale ordinaria presenta rischi giuridici, sanzionatori e di continuità estremi.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	n.d. / n.d. per 100	n.d./n.d.	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	n.d. / n.d. per milione	n.d./n.d.	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	n.d. / n.d.	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	n.d./100 - n.d.	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	n.d./100 - rank n.d.	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (12/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,4 / 4,1 / 6,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Ossezia del Sud, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 0/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Ossezia del Sud le evidenze principali sono nessun indicatore composito pienamente comparabile. La dimensione più robusta è maturità infrastrutturale (1,8/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (0,0/10). Sono disponibili 0 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata bassa. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Ossezia del Sud è 1,8/10. La base statistica rileva i principali dati WDI non sono disponibili in forma omogenea. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Per Ossezia del Sud non è disponibile un profilo Oxford Insights direttamente attribuibile; l'adozione di IA è quindi valutata attraverso GovTech, servizi online, infrastrutture e fonti qualitative. Il punteggio S2 è 1,5/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Ossezia del Sud è valutata fragile, con S3 pari a 0,0/10. Le evidenze disponibili comprendono evidenza quantitativa incompleta. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Ossezia del Sud ottiene S4 1,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Russia; l'indicatore di indipendenza disponibile è 1,8/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Ossezia del Sud, Dipendenza quasi totale da infrastrutture e fornitori russi. L'impatto sulla valutazione è misurato da S4=1,6/10 e dal proxy di indipendenza 1,8/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Ossezia del Sud è S5 1,5/10. La base ITU registra GCI non disponibile in forma comparabile. Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (12/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,4	Crimini finanziari	7,3
Reti criminali	5,6	Attori incorporati nello Stato	7,0
Attori stranieri	4,2	Attori del settore privato	7,0
Resilienza complessiva	4,1	Cooperazione internazionale	3,8
Politiche e norme nazionali	5,9	Forze dell'ordine	5,0
Antiriciclaggio	3,9	Prevenzione	4,0
Supporto vittime e testimoni	4,1	Rischio operativo FOTR-CY	6,8 - ALTO

Pressione del crimine digitale. Il profilo di Ossezia del Sud restituisce un rischio FOTR-CY di 6,8/10 (alto). La componente cyber-dipendente vale 7,4/10 e quella finanziaria 7,3/10; la risposta sistemica è valutata debole, con resilienza media di 4,1/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,0/10) e attori del settore privato (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Ossezia del Sud assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Ossezia del Sud, la resilienza complessiva è debole (4,1/10); la cooperazione internazionale è debole (3,8/10), le politiche e norme nazionali sono intermedie (5,9/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 3,9/10, prevenzione 4,0/10 e supporto a vittime e testimoni 4,1/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Ossezia del Sud, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; blocco di hosting e ASN ad alta reputazione negativa, ricerca proattiva delle minacce su malware sottrattori di informazioni e controllo dei canali RDP/VPN; verifica indipendente della proprietà e dei subfornitori. Poiché l'entità non dispone di una serie nazionale GI-TOC autonoma, i valori derivano da un proxy Celeborn Intelligence ponderato su Georgia 40%, Federazione Russa 60%; la confidenza deve pertanto essere considerata inferiore e la decisione resa più prudente.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; proxy Celeborn Intelligence ponderato su Georgia 40%, Federazione Russa 60%. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Ossezia del Sud, In Ossezia del Sud le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o

infrastrutture esterne. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Ossezia del Sud, Il livello governativo di Ossezia del Sud presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Ossezia del Sud, Sul piano militare e dual-use, Ossezia del Sud mostra forte integrazione o dipendenza dall'ecosistema russo, inclusi sistemi di comando, comunicazione e sicurezza. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Ossezia del Sud, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Ossezia del Sud, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 0,0/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
1,8	1,5	0,0	1,6	1,5	1,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
2,0	2,3	0,0	0,1	1,1	0,0

Il GCRI di Ossezia del Sud è 1,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 1,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Maturità cyber (2,3/10), mentre il più basso è Trasparenza istituzionale (0,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 1,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Ossezia del Sud, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Ossezia del Sud, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Ossezia del Sud, Dal punto di vista italiano, Ossezia del Sud rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Ossezia del Sud, il FOTR di 1,0/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

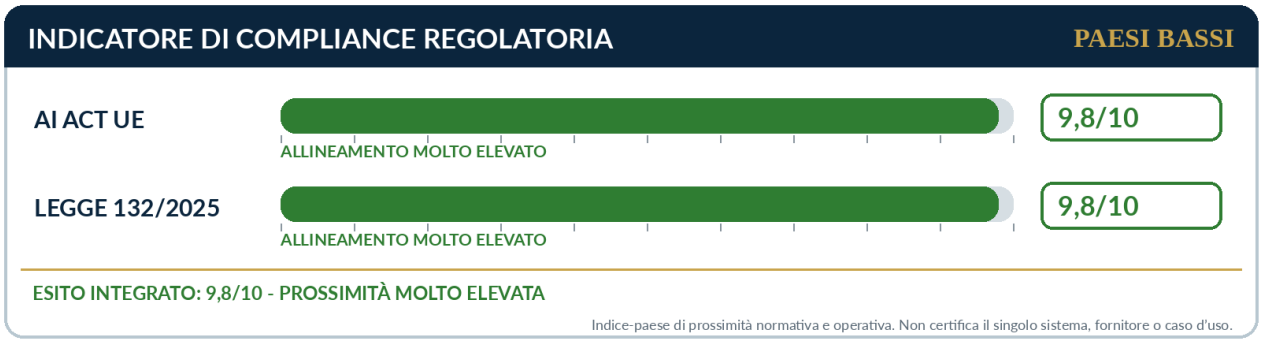
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Ossezia del Sud: World Development Indicators, valori più recenti disponibili 2022-2024; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Bassa con copertura 0/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Paesi Bassi

Posizione FOTR	6	Area	Europa	Subregione	Europa occidentale e centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	9,2	GCRI / 10	8,8	Classe operativa	Affidabilità molto alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Paesi Bassi, AI Act UE 9,8/10; legge 132/2025 9,8/10; esito integrato 9,8/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Per un operatore italiano, Paesi Bassi non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 97/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,8/10) e indice FOTR (9,2/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il sistema digitale di Paesi Bassi è avanzato e integrato con standard internazionali. Le principali criticità non sono di base istituzionale, ma riguardano supply chain, concentrazione dei servizi e gestione delle eccezioni di sicurezza nazionale.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	97,0% / 43,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 198.682 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	95,4 / 81,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	99,2/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	79,9/100 - rank 4	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	84/100 - Libero / Libero (97/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,0 / 7,4 / 5,3	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Paesi Bassi, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Paesi Bassi le evidenze principali sono GTMI 81,6/100, EGDI 95,4/100, GCI 99,2/100, AI readiness 79,9/100. La dimensione più robusta è maturità infrastrutturale (9,8/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (8,1/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Paesi Bassi è 9,8/10. La base statistica rileva utenti Internet pari al 97,0% nel 2024; 43,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 198.682 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Paesi Bassi al posto 4 con un valore medio di 79,9/100; il pilastro migliore è governance (94,2/100), quello più debole è sviluppo e diffusione (62,5/100). Il GTMI 2025 è 81,6/100. Il punteggio S2 è 8,1/10 e indica una capacità elevata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Paesi Bassi è valutata solida, con S3 pari a 8,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 96,9/100, sviluppo e diffusione dell'IA 62,5/100, penetrazione Internet 97,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Paesi Bassi ottiene S4 8,2/10 e presenta buona capacità di diversificazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 8,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Paesi Bassi, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario, luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=8,2/10 e dal proxy di indipendenza 8,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Paesi Bassi è S5 9,2/10. La base ITU registra ITU GCI 99,2/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è sviluppo delle capacità (19,2/20). Freedom on the Net è 84/100 - Libero, mentre Freedom in the World è Libero (97/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, Uitvoeringswet AVG, Computer Crime e disciplina nazionale NIS2; forte capacità di supervisione e resilienza digitale.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,0	Crimini finanziari	6,0
Reti criminali	6,5	Attori incorporati nello Stato	3,0
Attori stranieri	7,0	Attori del settore privato	4,5
Resilienza complessiva	7,4	Cooperazione internazionale	9,0
Politiche e norme nazionali	7,5	Forze dell'ordine	7,0
Antiriciclaggio	6,5	Prevenzione	8,0
Supporto vittime e testimoni	8,0	Rischio operativo FOTR-CY	5,3 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (7,0/10), criminalità finanziaria (6,0/10) e resilienza (7,4/10) colloca Paesi Bassi in una fascia di rischio significativo, pari a 5,3/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (7,0/10) e reti criminali (6,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Paesi Bassi assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Paesi Bassi, la resilienza complessiva è intermedia (7,4/10); la cooperazione internazionale è robusta (9,0/10), le politiche e norme nazionali sono robuste (7,5/10) e la capacità delle forze dell'ordine è intermedia (7,0/10). Completano il quadro antiriciclaggio 6,5/10, prevenzione 8,0/10 e supporto a vittime e testimoni 8,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Paesi Bassi, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Paesi Bassi. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Paesi Bassi, In Paesi Bassi le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. Per i

partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Paesi Bassi, Il livello governativo di Paesi Bassi presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Paesi Bassi, Sul piano militare e dual-use, Paesi Bassi mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Paesi Bassi, GDPR, Uitvoeringswet AVG, Computer Crime e disciplina nazionale NIS2; forte capacità di supervisione e resilienza digitale. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Paesi Bassi, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 10,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,8	8,1	8,6	8,2	9,2	8,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,8	8,5	8,5	10,0	8,4	10,0

Il GCRI di Paesi Bassi è 8,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 9,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (10,0/10), mentre il più basso è Supply chain (8,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Basso	Basso	Basso

La matrice applica il FOTR di 9,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Paesi Bassi, la matrice non individua ambiti ad alto rischio; 6 categorie risultano basse o medio-basse, ferma la verifica del singolo progetto. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Paesi Bassi, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Paesi Bassi, Dal punto di vista italiano, Paesi Bassi rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Paesi Bassi, il FOTR di 9,2/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (8,4/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

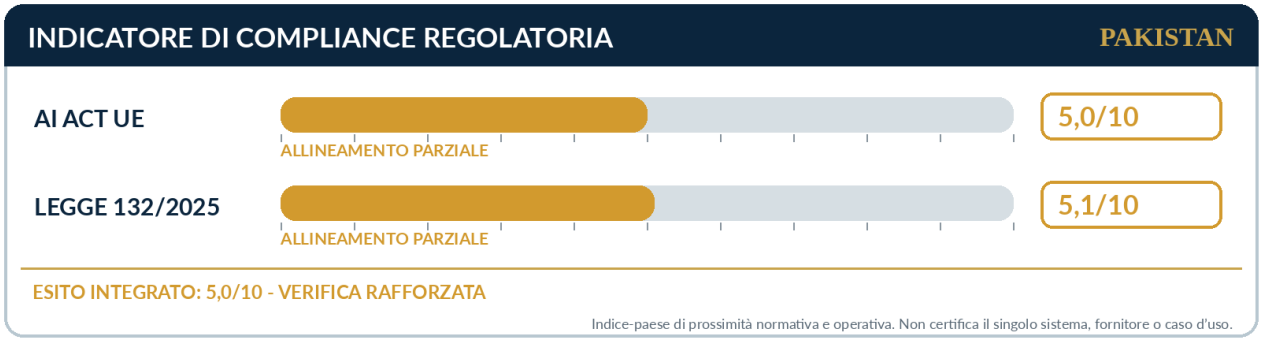
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Paesi Bassi: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Pakistan

Posizione FOTR	136	Area	Asia	Subregione	Asia meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,0	GCRI / 10	5,1	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Pakistan, AI Act UE 5,0/10; legge 132/2025 5,1/10; esito integrato 5,0/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Pakistan è stato membro delle nazioni unite collocato in Asia meridionale. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 32/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,1/10) e indice FOTR (5,0/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Pakistan presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	57,3% / 1,5 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	95,7% / 110 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	51,0 / 67,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	96,7/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	47,9/100 - rank 81	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	27/100 - Non libero / Parzialmente libero (32/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 4,0 / 6,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Pakistan, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Pakistan le evidenze principali sono GTMI 67,9/100, EGDI 51,0/100, GCI 96,7/100, AI readiness 47,9/100. La dimensione più robusta è postura di sicurezza cyber (6,9/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (4,2/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Pakistan è 4,7/10. La base statistica rileva utenti Internet pari al 57,3% nel 2024; 1,5 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 95,7% nel 2024; 110 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Pakistan al posto 81 con un valore medio di 47,9/100; il pilastro migliore è politiche pubbliche (61,5/100), quello più debole è adozione pubblica (36,5/100). Il GTMI 2025 è 67,9/100. Il punteggio S2 è 5,4/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Pakistan è valutata fragile, con S3 pari a 4,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 35,0/100, sviluppo e diffusione dell'IA 37,0/100, penetrazione Internet 57,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Pakistan ottiene S4 4,5/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina; l'indicatore di indipendenza disponibile è 3,6/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Pakistan, Forte presenza cinese nelle reti e nelle infrastrutture, con componenti statunitensi, europee e domestiche in segmenti selettivi. L'impatto sulla valutazione è misurato da S4=4,5/10 e dal proxy di indipendenza 3,6/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Pakistan è S5 6,9/10. La base ITU registra ITU GCI 96,7/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure tecniche (18,2/20). Freedom on the Net è 27/100 - Non libero, mentre Freedom in the World è Parzialmente libero (32/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	7,0
Reti criminali	7,0	Attori incorporati nello Stato	7,5
Attori stranieri	4,5	Attori del settore privato	5,0
Resilienza complessiva	4,0	Cooperazione internazionale	5,5
Politiche e norme nazionali	5,0	Forze dell'ordine	4,5
Antiriciclaggio	4,0	Prevenzione	4,0
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	6,0 - SIGNIFICATIVO

Quadro criminale digitale. Per Pakistan, l'indice operativo FOTR-CY è 6,0/10, classe significativa. Il mercato dei reati cyber-dipendenti è intermedio (5,0/10), mentre i crimini finanziari sono elevati (7,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,5/10) e reti criminali (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Pakistan assumono particolare rilevanza compromissione delle caselle di posta aziendale, frodi da call center, abuso di portafogli digitali mobili, identità sintetiche, ransomware, phishing bancario e triangolazioni transfrontaliere dei proventi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Pakistan, la resilienza complessiva è debole (4,0/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Pakistan, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Pakistan. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Pakistan, In Pakistan le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La disponibilità

del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Pakistan, Il livello governativo di Pakistan presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Pakistan, Sul piano militare e dual-use, Pakistan mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Pakistan, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Pakistan, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,2/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
4,7	5,4	4,2	4,5	6,9	5,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,8	5,7	4,9	5,1	5,3	4,2

Il GCRI di Pakistan è 5,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Maturità cyber (5,7/10), mentre il più basso è Trasferibilità dati (4,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 5,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Pakistan, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Pakistan, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Pakistan, Dal punto di vista italiano, Pakistan rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Pakistan è indicata una cooperazione selettiva, coerente con il FOTR di 5,0/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

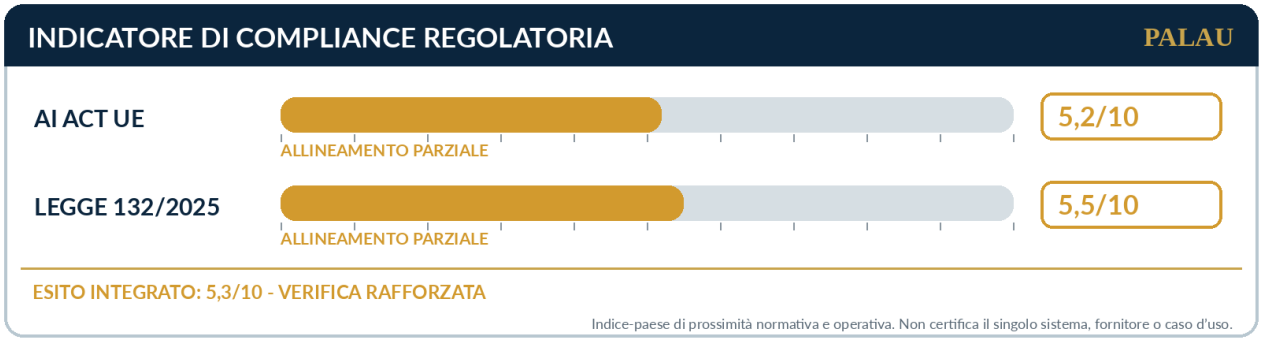
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Pakistan: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Palau

Posizione FOTR	116	Area	Oceania	Subregione	Pacifico insulare
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,5	GCRI / 10	4,5	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Palau, AI Act UE 5,2/10; legge 132/2025 5,5/10; esito integrato 5,3/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Oceania, Palau presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La distanza geografica e l'insularità rendono centrali cavi sottomarini, satelliti, continuità energetica e dipendenza da fornitori australiani, neozelandesi, statunitensi o asiatici. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 92/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,5/10) supera il GCRI tecnico (4,5/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Palau dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	83,9% / 7,3 per 100	2024/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 1.469 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	50,7 / 20,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	n.d./100 - n.d.	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	22,0/100 - rank 151	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (92/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 5,1 / 3,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Palau, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Palau le evidenze principali sono GTMI 20,6/100, EGDI 50,7/100, AI readiness 22,0/100. La dimensione più robusta è maturità infrastrutturale (6,0/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,4/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Palau è 6,0/10. La base statistica rileva utenti Internet pari al 83,9% nel 2024; 7,3 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 100,0% nel 2024; 1.469 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Palau al posto 151 con un valore medio di 22,0/100; il pilastro migliore è infrastrutture IA (41,5/100), quello più debole è politiche pubbliche (4,0/100). Il GTMI 2025 è 20,6/100. Il punteggio S2 è 2,4/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Palau è valutata fragile, con S3 pari a 4,9/10. Le evidenze disponibili comprendono indice UN di capitale umano 75,2/100, sviluppo e diffusione dell'IA 20,0/100, penetrazione Internet 83,9%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Palau ottiene S4 4,0/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Palau, Dipendenza da Australia, Nuova Zelanda, Stati Uniti, Francia e operatori satellitari o sottomarini; la scala ridotta limita la diversificazione e aumenta il rischio di concentrazione. L'impatto sulla

valutazione è misurato da S4=4,0/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Palau è S5 5,3/10. La base ITU registra GCI non disponibile in forma comparabile. Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (92/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	3,0
Reti criminali	4,0	Attori incorporati nello Stato	3,5
Attori stranieri	4,0	Attori del settore privato	2,0
Resilienza complessiva	5,1	Cooperazione internazionale	7,0
Politiche e norme nazionali	5,5	Forze dell'ordine	5,0
Antiriciclaggio	4,5	Prevenzione	5,0
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	3,7 - MODERATO

Sintesi del rischio cybercrime. Palau presenta un'esposizione stimata moderata (3,7/10): reati cyber-dipendenti 3,0/10, crimini finanziari 3,0/10 e resilienza 5,1/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (4,0/10) e attori stranieri (4,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Palau assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Palau, la resilienza complessiva è debole (5,1/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 5,0/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Palau, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Palau. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Palau, In Palau le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Palau, Il livello governativo di Palau presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il

settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Palau, Sul piano militare e dual-use, Palau mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Palau, Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Palau, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,0/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,0	2,4	4,9	4,0	5,3	4,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,6	4,9	6,1	6,5	4,7	5,0

Il GCRI di Palau è 4,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,5/10), mentre il più basso è Supply chain (4,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio	Medio-alto	Medio	Medio	Medio

La matrice applica il FOTR di 5,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Palau, 2 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Cloud e infrastrutture. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Palau, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Palau, Dal punto di vista italiano, Palau rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Palau è indicata una cooperazione selettiva, coerente con il FOTR di 5,5/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

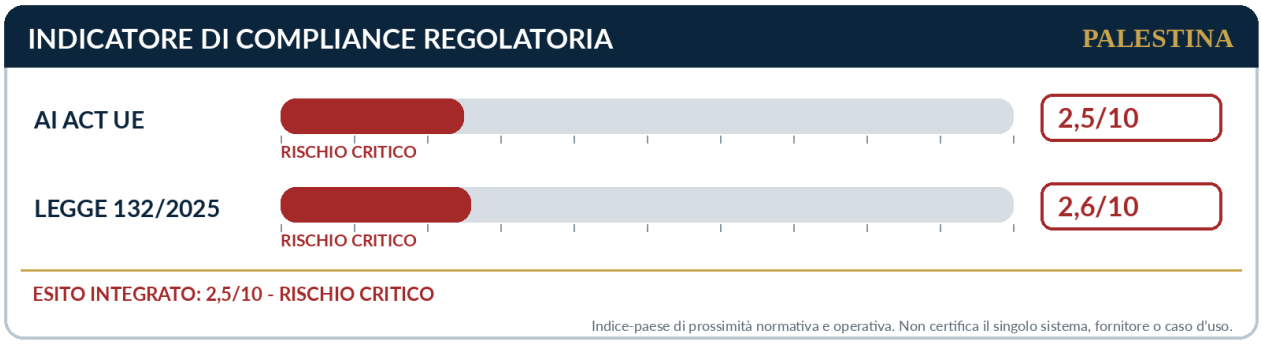
Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Palau: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Palestina

Posizione FOTR	188	Area	Asia	Subregione	Medio Oriente e Asia occidentale
Status	Stato osservatore permanente presso le Nazioni Unite	Confidenza Celeborn Intelligence	Media	Copertura dati	4/7 famiglie
FOTR / 10	2,4	GCRI / 10	3,4	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Palestina, AI Act UE 2,5/10; legge 132/2025 2,6/10; esito integrato 2,5/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Palestina, situato in Medio Oriente e Asia occidentale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Per questa entità non è disponibile un indicatore Freedom in the World direttamente comparabile; l'assenza di copertura viene trattata come limite informativo e non come prova automatica di rischio. Il GCRI tecnico (3,4/10) è superiore al punteggio FOTR (2,4/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Il rapporto digitale con Palestina deve essere considerato eccezionale e ad alta esposizione. Sono necessari screening sanzionatori, autorizzazioni, segregazione completa e impossibilità tecnica di accedere ai dati in chiaro.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	86,6% / 8,2 per 100	2023/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 427 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	n.d. / n.d.	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	n.d./100 - n.d.	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	33,8/100 - rank 115	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / n.d.	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 4,3 / 6,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Palestina, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 4/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Palestina le evidenze principali sono AI readiness 33,8/100. La dimensione più robusta è maturità infrastrutturale (6,0/10), mentre la criticità relativa riguarda postura di sicurezza cyber (1,5/10). Sono disponibili 4 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata media. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Palestina è 6,0/10. La base statistica rileva utenti Internet pari al 86,6% nel 2023; 8,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 427 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Palestina al posto 115 con un valore medio di 33,8/100; il pilastro migliore è adozione pubblica (44,6/100), quello più debole è resilienza (17,1/100). Il punteggio S2 è 3,5/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Palestina è valutata fragile, con S3 pari a 2,8/10. Le evidenze disponibili comprendono sviluppo e diffusione dell'IA 37,6/100, penetrazione Internet 86,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Palestina ottiene S4 3,4/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Palestina, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo

societario e subfornitura. L'impatto sulla valutazione è misurato da S4=3,4/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Palestina è S5 1,5/10. La base ITU registra GCI non disponibile in forma comparabile. Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è n.d.. Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	7,8
Reti criminali	6,9	Attori incorporati nello Stato	7,8
Attori stranieri	6,4	Attori del settore privato	6,1
Resilienza complessiva	4,3	Cooperazione internazionale	6,4
Politiche e norme nazionali	5,0	Forze dell'ordine	4,7
Antiriciclaggio	4,9	Prevenzione	4,5
Supporto vittime e testimoni	3,8	Rischio operativo FOTR-CY	6,4 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Palestina restituisce un rischio FOTR-CY di 6,4/10 (significativo). La componente cyber-dipendente vale 4,5/10 e quella finanziaria 7,8/10; la risposta sistemica è valutata debole, con resilienza media di 4,3/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,8/10) e reti criminali (6,9/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Palestina assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Palestina, la resilienza complessiva è debole (4,3/10); la cooperazione internazionale è intermedia (6,4/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è debole (4,7/10). Completano il quadro antiriciclaggio 4,9/10, prevenzione 4,5/10 e supporto a vittime e testimoni 3,8/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Palestina, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative. Poiché l'entità non dispone di una serie nazionale GI-TOC autonoma, i valori derivano da un proxy Celeborn Intelligence ponderato su Giordania 40%, Libano 35%, Egitto 25%; la confidenza deve pertanto essere considerata inferiore e la decisione resa più prudente.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; proxy Celeborn Intelligence ponderato su Giordania 40%, Libano 35%, Egitto 25%. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Palestina, In Palestina le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Palestina, Il livello governativo di Palestina presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Palestina, Sul piano militare e dual-use, Palestina mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Palestina, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Palestina, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 1,6/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,0	3,5	2,8	3,4	1,5	3,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
3,0	2,4	2,2	2,9	2,0	1,6

Il GCRI di Palestina è 3,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 2,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (3,0/10), mentre il più basso è Trasferibilità dati (1,6/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Alto	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 2,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Palestina, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Palestina, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Palestina, Dal punto di vista italiano, Palestina rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Palestina, il FOTR di 2,4/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

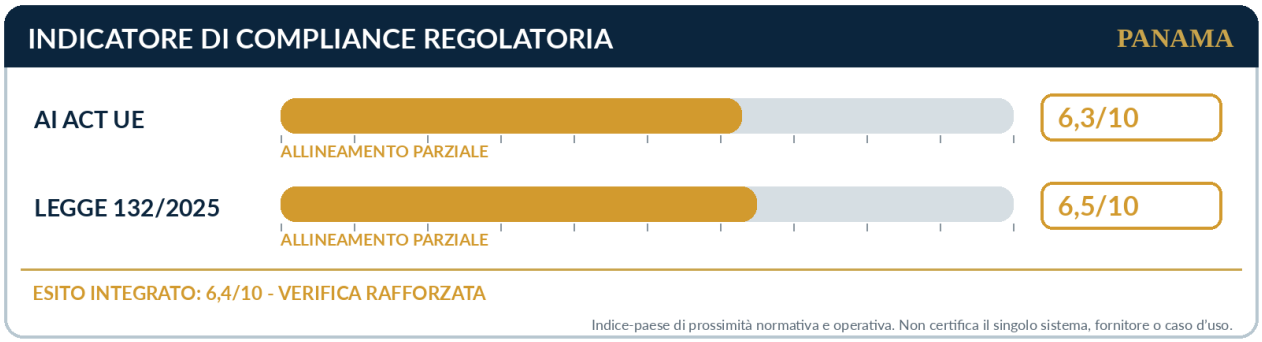
Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.
Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.
Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Palestina: World Development Indicators, valori più recenti disponibili 2022-2024; Oxford Insights Government AI Readiness Index 2025; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Media con copertura 4/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Panama

Posizione FOTR	58	Area	Americhe	Subregione	America centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	6,5	GCRI / 10	6,0	Classe operativa	Affidabilità favorevole ma condizionata

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Panama, AI Act UE 6,3/10; legge 132/2025 6,5/10; esito integrato 6,4/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Panama non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 82/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,0/10) e indice FOTR (6,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il quadro di Panama è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	72,8% / 18,1 per 100	2024/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	96,0% / 2.234 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	73,0 / 76,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	66,5/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	38,4/100 - rank 102	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (82/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,0 / 4,7 / 6,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Panama, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Panama le evidenze principali sono GTMI 76,2/100, EGDI 73,0/100, GCI 66,5/100, AI readiness 38,4/100. La dimensione più robusta è maturità infrastrutturale (7,4/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (5,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Panama è 7,4/10. La base statistica rileva utenti Internet pari al 72,8% nel 2024; 18,1 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 96,0% nel 2024; 2.234 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Panama al posto 102 con un valore medio di 38,4/100; il pilastro migliore è adozione pubblica (61,3/100), quello più debole è sviluppo e diffusione (20,8/100). Il GTMI 2025 è 76,2/100. Il punteggio S2 è 5,1/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Panama è valutata sufficiente ma disomogenea, con S3 pari a 5,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 68,7/100, sviluppo e diffusione dell'IA 20,8/100, penetrazione Internet 72,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Panama ottiene S4 5,8/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Panama, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=5,8/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Panama è S5 6,6/10. La base ITU registra ITU GCI 66,5/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (7,1/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (82/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge 81/2019 sulla protezione dei dati e normativa di commercio elettronico; trasferimenti UE mediante garanzie appropriate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,0	Crimini finanziari	7,5
Reti criminali	7,0	Attori incorporati nello Stato	7,5
Attori stranieri	6,5	Attori del settore privato	8,0
Resilienza complessiva	4,7	Cooperazione internazionale	6,0
Politiche e norme nazionali	6,0	Forze dell'ordine	4,5
Antiriciclaggio	3,5	Prevenzione	4,5
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	6,6 - ALTO

Rischio criminale connesso alle tecnologie. In Panama il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 6,6/10, livello alto. I reati che dipendono direttamente da sistemi informatici raggiungono 7,0/10; le frodi e i reati finanziari 7,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori del settore privato (8,0/10) e attori incorporati nello Stato (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Panama assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Panama, la resilienza complessiva è debole (4,7/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 4,5/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Panama, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Panama. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Panama, In Panama le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio

comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Panama, Il livello governativo di Panama presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Panama, Sul piano militare e dual-use, Panama mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Panama, Legge 81/2019 sulla protezione dei dati e normativa di commercio elettronico; trasferimenti UE mediante garanzie appropriate. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Panama, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 6,1/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,4	5,1	5,2	5,8	6,6	6,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,7	6,5	6,3	6,7	6,5	6,1

Il GCRI di Panama è 6,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (6,7/10), mentre il più basso è Trasferibilità dati (6,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Panama, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Panama, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Panama, Dal punto di vista italiano, Panama rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Panama è favorevole ma condizionata: il valore FOTR di 6,5/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Trasferibilità dati.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

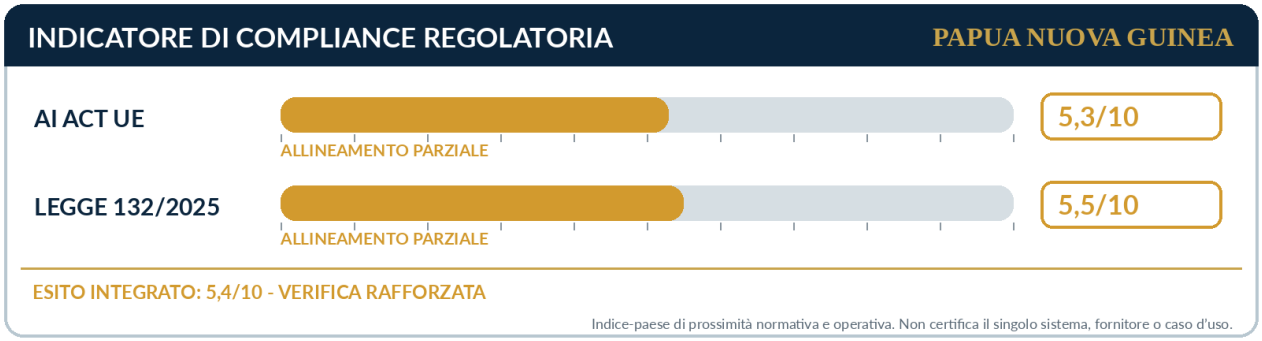
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Panama: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Papua Nuova Guinea

Posizione FOTR	117	Area	Oceania	Subregione	Pacifico insulare
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,5	GCRI / 10	3,9	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Papua Nuova Guinea, AI Act UE 5,3/10; legge 132/2025 5,5/10; esito integrato 5,4/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Papua Nuova Guinea è stato membro delle nazioni unite collocato in Pacifico insulare. La distanza geografica e l'insularità rendono centrali cavi sottomarini, satelliti, continuità energetica e dipendenza da fornitori australiani, neozelandesi, statunitensi o asiatici. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 61/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,5/10) supera il GCRI tecnico (3,9/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il quadro di Papua Nuova Guinea è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	18,8% / 0,2 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	43,3% / 88 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	30,8 / 54,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	62,6/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	28,1/100 - rank 135	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (61/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,0 / 3,2 / 6,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Papua Nuova Guinea, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Papua Nuova Guinea le evidenze principali sono GTMI 54,8/100, EGDI 30,8/100, GCI 62,6/100, AI readiness 28,1/100. La dimensione più robusta è postura di sicurezza cyber (5,9/10), mentre la criticità relativa riguarda maturità infrastrutturale (2,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Papua Nuova Guinea è 2,1/10. La base statistica rileva utenti Internet pari al 18,8% nel 2024; 0,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 43,3% nel 2024; 88 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Papua Nuova Guinea al posto 135 con un valore medio di 28,1/100; il pilastro migliore è adozione pubblica (43,0/100), quello più debole è politiche pubbliche (15,5/100). Il GTMI 2025 è 54,8/100. Il punteggio S2 è 3,4/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Papua Nuova Guinea è valutata fragile, con S3 pari a 3,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 39,8/100, sviluppo e diffusione dell'IA 19,3/100, penetrazione Internet 18,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Papua Nuova Guinea ottiene S4 4,5/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Papua Nuova Guinea, Dipendenza da Australia, Nuova Zelanda, Stati Uniti, Francia e operatori satellitari o sottomarini; la scala ridotta limita la diversificazione e aumenta il rischio di concentrazione.

L'impatto sulla valutazione è misurato da S4=4,5/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Papua Nuova Guinea è S5 5,9/10. La base ITU registra ITU GCI 62,6/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (9,3/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (61/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,0	Crimini finanziari	8,5
Reti criminali	8,0	Attori incorporati nello Stato	8,5
Attori stranieri	6,5	Attori del settore privato	6,5
Resilienza complessiva	3,2	Cooperazione internazionale	4,5
Politiche e norme nazionali	5,5	Forze dell'ordine	3,0
Antiriciclaggio	3,5	Prevenzione	2,5
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	6,5 - ALTO

Quadro criminale digitale. Per Papua Nuova Guinea, l'indice operativo FOTR-CY è 6,5/10, classe alta. Il mercato dei reati cyber-dipendenti è intermedio (4,0/10), mentre i crimini finanziari sono molto elevati (8,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,5/10) e reti criminali (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Papua Nuova Guinea assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Papua Nuova Guinea, la resilienza complessiva è molto debole (3,2/10); la cooperazione internazionale è debole (4,5/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è molto debole (3,0/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 2,5/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Papua Nuova Guinea, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Papua Nuova Guinea. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Papua Nuova Guinea, In Papua Nuova Guinea le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Papua Nuova Guinea, Il livello governativo di Papua Nuova Guinea presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Papua Nuova Guinea, Sul piano militare e dual-use, Papua Nuova Guinea mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Papua Nuova Guinea, Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Papua Nuova Guinea, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,0/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
2,1	3,4	3,6	4,5	5,9	3,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,6	5,2	5,7	6,2	5,3	5,0

Il GCRI di Papua Nuova Guinea è 3,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,2/10), mentre il più basso è Trasferibilità dati (5,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio	Medio-alto	Medio	Medio	Medio

La matrice applica il FOTR di 5,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Papua Nuova Guinea, 2 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Cloud e infrastrutture. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Papua Nuova Guinea, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Papua Nuova Guinea, Dal punto di vista italiano, Papua Nuova Guinea rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA,

audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Papua Nuova Guinea è indicata una cooperazione selettiva, coerente con il FOTR di 5,5/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

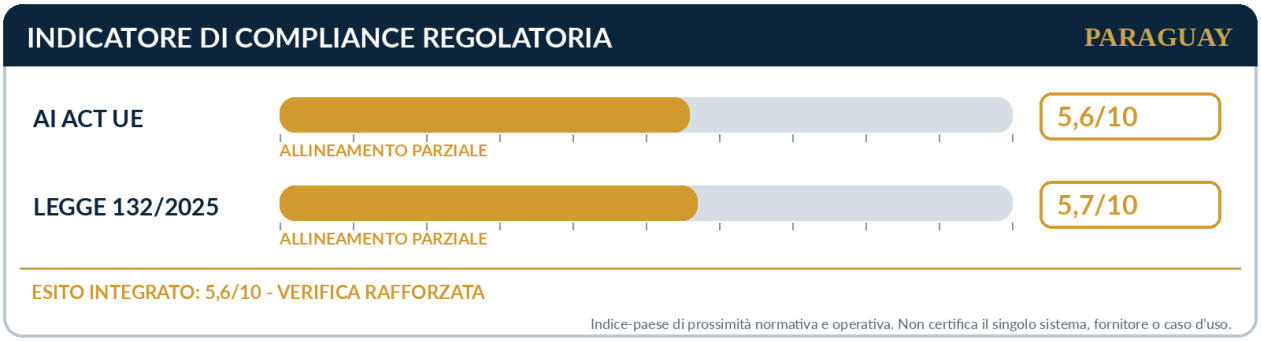
Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Papua Nuova Guinea: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Paraguay

Posizione FOTR	101	Area	Americhe	Subregione	America meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,7	GCRI / 10	5,9	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Paraguay, AI Act UE 5,6/10; legge 132/2025 5,7/10; esito integrato 5,6/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Americhe, Paraguay presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 63/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,9/10) e indice FOTR (5,7/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il quadro di Paraguay è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	81,6% / 12,9 per 100	2024/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	99,8% / 775 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	72,5 / 71,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	74,8/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	36,2/100 - rank 111	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (63/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,5 / 3,3 / 7,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Paraguay, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Paraguay le evidenze principali sono GTMI 71,8/100, EGDI 72,5/100, GCI 74,8/100, AI readiness 36,2/100. La dimensione più robusta è maturità infrastrutturale (7,1/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,8/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Paraguay è 7,1/10. La base statistica rileva utenti Internet pari al 81,6% nel 2024; 12,9 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 99,8% nel 2024; 775 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Paraguay al posto 111 con un valore medio di 36,2/100; il pilastro migliore è governance (55,3/100), quello più debole è politiche pubbliche (12,0/100). Il GTMI 2025 è 71,8/100. Il punteggio S2 è 4,8/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Paraguay è valutata sufficiente ma disomogenea, con S3 pari a 5,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 70,9/100, sviluppo e diffusione dell'IA 19,1/100, penetrazione Internet 81,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Paraguay ottiene S4 5,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Paraguay, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=5,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Paraguay è S5 6,8/10. La base ITU registra ITU GCI 74,8/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (8,5/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (63/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,5	Crimini finanziari	7,5
Reti criminali	8,0	Attori incorporati nello Stato	9,0
Attori stranieri	9,0	Attori del settore privato	8,0
Resilienza complessiva	3,3	Cooperazione internazionale	6,5
Politiche e norme nazionali	3,5	Forze dell'ordine	2,0
Antiriciclaggio	2,5	Prevenzione	3,5
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	7,4 - ALTO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (6,5/10), criminalità finanziaria (7,5/10) e resilienza (3,3/10) colloca Paraguay in una fascia di rischio alto, pari a 7,4/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e attori stranieri (9,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Paraguay assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Paraguay, la resilienza complessiva è molto debole (3,3/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono deboli (3,5/10) e la capacità delle forze dell'ordine è molto debole (2,0/10). Completano il quadro antiriciclaggio 2,5/10, prevenzione 3,5/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Paraguay, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Paraguay. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Paraguay, In Paraguay le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Paraguay, Il livello governativo di Paraguay presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Paraguay, Sul piano militare e dual-use, Paraguay mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Paraguay, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Paraguay, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,4/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,1	4,8	5,4	5,3	6,8	5,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,8	5,5	5,5	6,2	5,6	5,4

Il GCRI di Paraguay è 5,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,2/10), mentre il più basso è Trasferibilità dati (5,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Paraguay, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Paraguay, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Paraguay, Dal punto di vista italiano, Paraguay rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Paraguay è indicata una cooperazione selettiva, coerente con il FOTR di 5,7/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasferibilità dati a decisione caso per caso.

Presidi minimi raccomandati

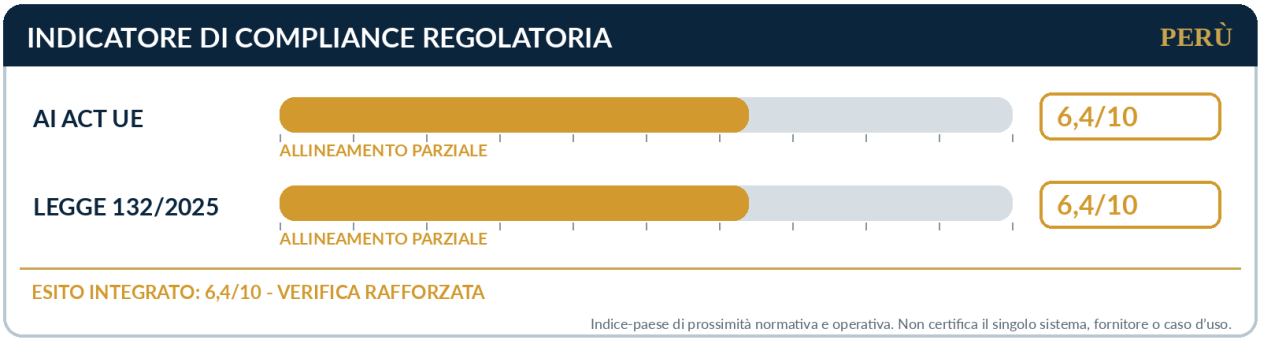
Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Paraguay: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Perù

Posizione FOTR	64	Area	Americhe	Subregione	America meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	6,3	GCRI / 10	6,7	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Perù, AI Act UE 6,4/10; legge 132/2025 6,4/10; esito integrato 6,4/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Perù, situato in America meridionale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 66/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,7/10) e indice FOTR (6,3/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il quadro di Perù è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	82,0% / 11,7 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	96,5% / 827 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	80,7 / 92,1	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	83,7/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	61,3/100 - rank 60	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (66/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 4,5 / 6,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Perù, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Perù le evidenze principali sono GTMI 92,1/100, EGDI 80,7/100, GCI 83,7/100, AI readiness 61,3/100. La dimensione più robusta è postura di sicurezza cyber (7,5/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,8/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Perù è 7,2/10. La base statistica rileva utenti Internet pari al 82,0% nel 2024; 11,7 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 96,5% nel 2024; 827 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Perù al posto 60 con un valore medio di 61,3/100; il pilastro migliore è adozione pubblica (90,4/100), quello più debole è sviluppo e diffusione (31,6/100). Il GTMI 2025 è 92,1/100. Il punteggio S2 è 6,9/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Perù è valutata sufficiente ma disomogenea, con S3 pari a 6,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 74,7/100, sviluppo e diffusione dell'IA 31,6/100, penetrazione Internet 82,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Perù ottiene S4 5,8/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Perù, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=5,8/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Perù è S5 7,5/10. La base ITU registra ITU GCI 83,7/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (13,5/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (66/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge 29733 e regolamento sulla protezione dei dati; disciplina di governo digitale e sicurezza in evoluzione.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	6,0
Reti criminali	8,5	Attori incorporati nello Stato	8,0
Attori stranieri	6,5	Attori del settore privato	4,5
Resilienza complessiva	4,5	Cooperazione internazionale	5,5
Politiche e norme nazionali	6,0	Forze dell'ordine	4,0
Antiriciclaggio	4,5	Prevenzione	3,5
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	6,1 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (5,0/10), criminalità finanziaria (6,0/10) e resilienza (4,5/10) colloca Perù in una fascia di rischio significativo, pari a 6,1/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (8,5/10) e attori incorporati nello Stato (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Perù assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Perù, la resilienza complessiva è debole (4,5/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 3,5/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Perù, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Perù. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Perù, In Perù le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Perù, Il livello governativo di Perù presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Perù, Sul piano militare e dual-use, Perù mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Perù, Legge 29733 e regolamento sulla protezione dei dati; disciplina di governo digitale e sicurezza in evoluzione. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Perù, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 6,3/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,2	6,9	6,2	5,8	7,5	6,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,6	6,0	6,2	6,4	6,4	6,3

Il GCRI di Perù è 6,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,3/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (6,6/10), mentre il più basso è Maturità cyber (6,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,3/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Perù, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Perù, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Perù, Dal punto di vista italiano, Perù rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Perù è indicata una cooperazione selettiva, coerente con il FOTR di 6,3/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Maturità cyber a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

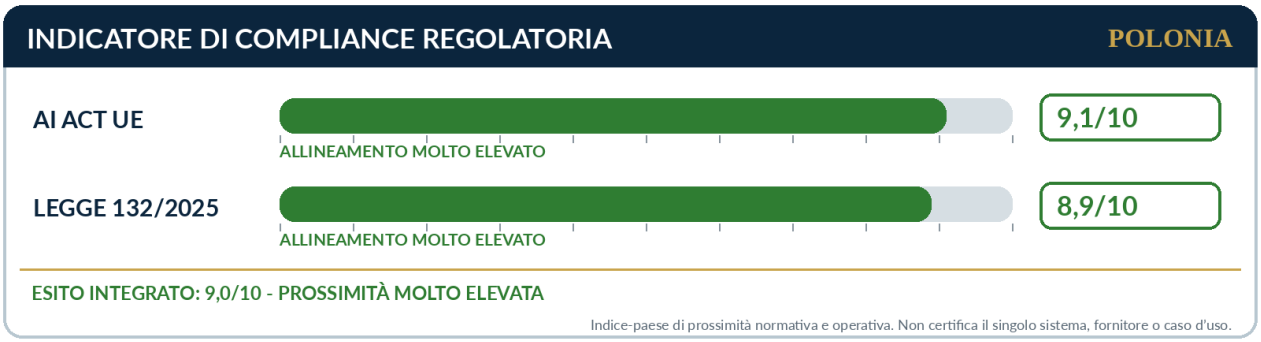
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Perù: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Polonia

Posizione FOTR	32	Area	Europa	Subregione	Europa occidentale e centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,2	GCRI / 10	7,6	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Polonia, AI Act UE 9,1/10; legge 132/2025 8,9/10; esito integrato 9,0/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Per un operatore italiano, Polonia non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 82/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,6/10) e indice FOTR (8,2/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ambiente digitale di Polonia è complessivamente affidabile e aperto agli scambi. Per investimenti italiani è opportuno verificare la disciplina locale, la struttura dei fornitori e gli eventuali poteri pubblici di accesso.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	88,6% / 25,4 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 41.132 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	86,5 / 67,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	93,5/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	73,9/100 - rank 24	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (82/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,0 / 6,1 / 5,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Polonia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Polonia le evidenze principali sono GTMI 67,0/100, EGDI 86,5/100, GCI 93,5/100, AI readiness 73,9/100. La dimensione più robusta è maturità infrastrutturale (8,8/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,0/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Polonia è 8,8/10. La base statistica rileva utenti Internet pari al 88,6% nel 2024; 25,4 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 41.132 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Polonia al posto 24 con un valore medio di 73,9/100; il pilastro migliore è politiche pubbliche (96,0/100), quello più debole è sviluppo e diffusione (47,2/100). Il GTMI 2025 è 67,0/100. Il punteggio S2 è 7,2/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Polonia è valutata sufficiente ma disomogenea, con S3 pari a 7,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 83,0/100, sviluppo e diffusione dell'IA 47,2/100, penetrazione Internet 88,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Polonia ottiene S4 6,0/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Polonia, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,0/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Polonia è S5 8,7/10. La base ITU registra ITU GCI 93,5/100, Tier 2 - avanzato; il pilastro relativamente più debole è organizzazione (16,7/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (82/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, Personal Data Protection Act, National Cybersecurity System Act e recepimento NIS2.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,0	Crimini finanziari	6,0
Reti criminali	6,0	Attori incorporati nello Stato	4,5
Attori stranieri	4,0	Attori del settore privato	4,5
Resilienza complessiva	6,1	Cooperazione internazionale	7,5
Politiche e norme nazionali	7,0	Forze dell'ordine	6,5
Antiriciclaggio	6,5	Prevenzione	6,0
Supporto vittime e testimoni	5,5	Rischio operativo FOTR-CY	5,1 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Polonia presenta un'esposizione stimata significativa (5,1/10): reati cyber-dipendenti 6,0/10, crimini finanziari 6,0/10 e resilienza 6,1/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (6,0/10) e attori incorporati nello Stato (4,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Polonia assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Polonia, la resilienza complessiva è intermedia (6,1/10); la cooperazione internazionale è robusta (7,5/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è intermedia (6,5/10). Completano il quadro antiriciclaggio 6,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 5,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Polonia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Polonia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Polonia, In Polonia le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Polonia, Il livello governativo di Polonia presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Polonia, Sul piano militare e dual-use, Polonia mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Polonia, GDPR, Personal Data Protection Act, National Cybersecurity System Act e recepimento NIS2. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Polonia, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,2/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,8	7,2	7,4	6,0	8,7	7,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,8	7,6	7,8	8,7	7,1	9,2

Il GCRI di Polonia è 7,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,2/10), mentre il più basso è Supply chain (7,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Polonia, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Polonia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Polonia, Dal punto di vista italiano, Polonia rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Polonia, il FOTR di 8,2/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (7,1/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

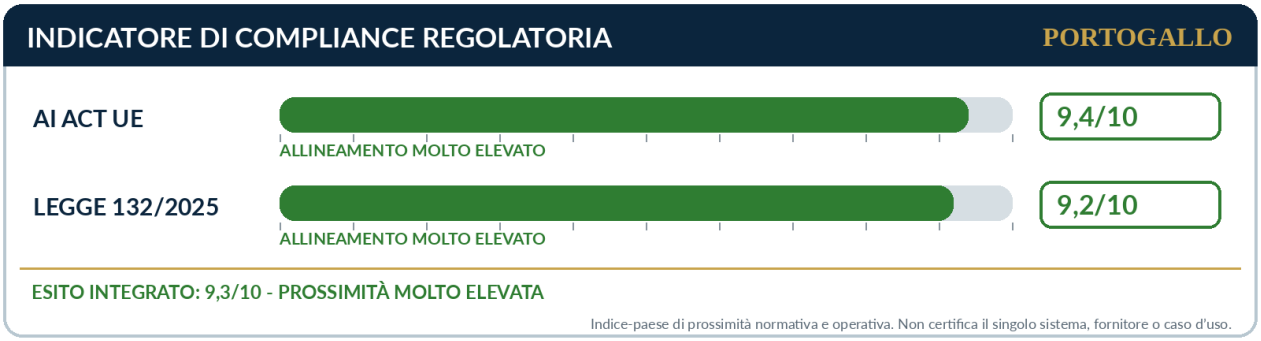
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Polonia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Portogallo

Posizione FOTR	23	Area	Europa	Subregione	Europa meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,6	GCRI / 10	7,9	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Portogallo, AI Act UE 9,4/10; legge 132/2025 9,2/10; esito integrato 9,3/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Portogallo è stato membro delle nazioni unite collocato in Europa meridionale. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 96/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,9/10) e indice FOTR (8,6/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il sistema digitale di Portogallo è avanzato e integrato con standard internazionali. Le principali criticità non sono di base istituzionale, ma riguardano supply chain, concentrazione dei servizi e gestione delle eccezioni di sicurezza nazionale.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	88,5% / 45,2 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 28.710 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	84,2 / 90,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	99,9/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	68,5/100 - rank 28	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (96/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 6,6 / 4,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Portogallo, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Portogallo le evidenze principali sono GTMI 90,0/100, EGDI 84,2/100, GCI 99,9/100, AI readiness 68,5/100. La dimensione più robusta è postura di sicurezza cyber (9,4/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Portogallo è 9,2/10. La base statistica rileva utenti Internet pari al 88,5% nel 2024; 45,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 28.710 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Portogallo al posto 28 con un valore medio di 68,5/100; il pilastro migliore è governance (93,5/100), quello più debole è sviluppo e diffusione (52,9/100). Il GTMI 2025 è 90,0/100. Il punteggio S2 è 7,3/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Portogallo è valutata sufficiente ma disomogenea, con S3 pari a 7,7/10. Le evidenze disponibili comprendono indice UN di capitale umano 83,9/100, sviluppo e diffusione dell'IA 52,9/100, penetrazione Internet 88,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Portogallo ottiene S4 6,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Portogallo, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo

societario, luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Portogallo è S5 9,4/10. La base ITU registra ITU GCI 99,9/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è sviluppo delle capacità (19,9/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (96/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, legge 58/2019 e disciplina nazionale di cybersicurezza; corpus UE integralmente applicabile.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	5,0
Reti criminali	6,0	Attori incorporati nello Stato	4,5
Attori stranieri	6,0	Attori del settore privato	5,0
Resilienza complessiva	6,6	Cooperazione internazionale	8,0
Politiche e norme nazionali	7,0	Forze dell'ordine	7,0
Antiriciclaggio	6,5	Prevenzione	6,0
Supporto vittime e testimoni	7,0	Rischio operativo FOTR-CY	4,9 - MODERATO

Rischio criminale connesso alle tecnologie. In Portogallo il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 4,9/10, livello moderato. I reati che dipendono direttamente da sistemi informatici raggiungono 5,5/10; le frodi e i reati finanziari 5,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (6,0/10) e attori stranieri (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Portogallo assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Portogallo, la resilienza complessiva è intermedia (6,6/10); la cooperazione internazionale è robusta (8,0/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è intermedia (7,0/10). Completano il quadro antiriciclaggio 6,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 7,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Portogallo, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Portogallo. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Portogallo, In Portogallo le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Portogallo, Il livello governativo di Portogallo presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Portogallo, Sul piano militare e dual-use, Portogallo mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Portogallo, GDPR, legge 58/2019 e disciplina nazionale di cybersicurezza; corpus UE integralmente applicabile. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Portogallo, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,3/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,2	7,3	7,7	6,1	9,4	7,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,9	8,3	8,1	9,2	7,3	9,3

Il GCRI di Portogallo è 7,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,3/10), mentre il più basso è Supply chain (7,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Portogallo, la cautela si concentra su 4 ambiti a rischio intermedio: Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Portogallo, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Portogallo, Dal punto di vista italiano, Portogallo rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Portogallo, il FOTR di 8,6/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (7,3/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

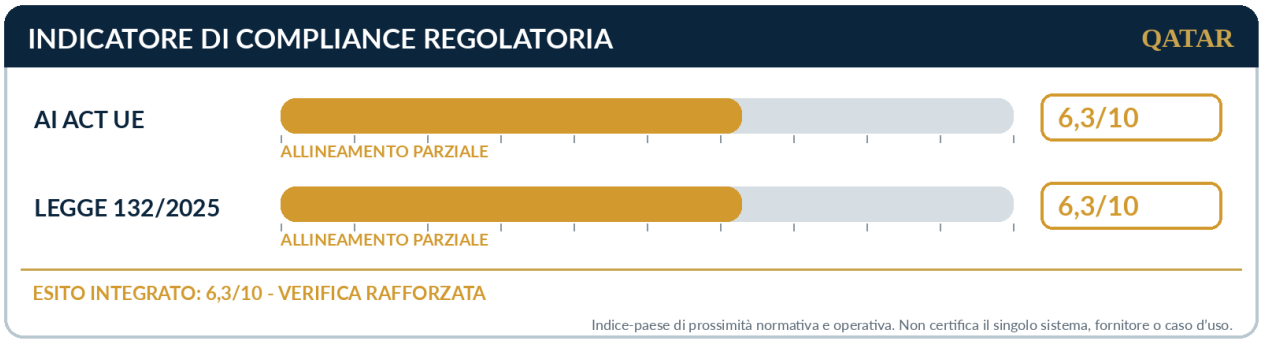
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Portogallo: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Qatar

Posizione FOTR	**68**	**Area**	Asia	**Subregione**	Medio Oriente e Asia occidentale
Status	**Stato membro delle Nazioni Unite**	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	**6,2**	**GCRI / 10**	**7,1**	**Classe operativa**	**Affidabilità selettiva**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Qatar, AI Act UE 6,3/10; legge 132/2025 6,3/10; esito integrato 6,3/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Asia, Qatar presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 25/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,1/10) e indice FOTR (6,2/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Qatar dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	98,1% / 11,8 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 445 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	82,4 / 86,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	100,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	60,4/100 - rank 54	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (25/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,5 / 5,5 / 6,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Qatar, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Qatar le evidenze principali sono GTMI 86,4/100, EGDI 82,4/100, GCI 100,0/100, AI readiness 60,4/100. La dimensione più robusta è postura di sicurezza cyber (8,7/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,8/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Qatar è 8,1/10. La base statistica rileva utenti Internet pari al 98,1% nel 2024; 11,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 445 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Qatar al posto 54 con un valore medio di 60,4/100; il pilastro migliore è politiche pubbliche (80,5/100), quello più debole è resilienza (39,0/100). Il GTMI 2025 è 86,4/100. Il punteggio S2 è 6,7/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Qatar è valutata sufficiente ma disomogenea, con S3 pari a 6,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 71,1/100, sviluppo e diffusione dell'IA 44,5/100, penetrazione Internet 98,1%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Qatar ottiene S4 5,8/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Qatar, Prevalenza statunitense ed europea nei sistemi critici e di difesa, con presenza asiatica nelle reti commerciali. L'impatto sulla valutazione è misurato da S4=5,8/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Qatar è S5 8,7/10. La base ITU registra ITU GCI 100,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure giuridiche (20,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (25/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Legge 13/2016 sulla protezione dei dati e regimi QFC; quadro cyber centralizzato, con necessità di valutare accessi pubblici e legge applicabile.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,5	Crimini finanziari	7,5
Reti criminali	6,0	Attori incorporati nello Stato	6,5
Attori stranieri	6,0	Attori del settore privato	6,0
Resilienza complessiva	5,5	Cooperazione internazionale	6,5
Politiche e norme nazionali	5,0	Forze dell'ordine	5,0
Antiriciclaggio	5,5	Prevenzione	6,0
Supporto vittime e testimoni	5,5	Rischio operativo FOTR-CY	6,1 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Qatar il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 6,1/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 6,5/10; le frodi e i reati finanziari 7,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (6,5/10) e reti criminali (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Qatar assumono particolare rilevanza phishing e credential theft, ransomware, frodi d'investimento, attacchi a energia e servizi pubblici, abuso di cripto-attività e campagne che possono combinare profitto, spionaggio e pressione politica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Qatar, la resilienza complessiva è debole (5,5/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 5,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Qatar, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Qatar. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Qatar, In Qatar le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Qatar, Il livello governativo di Qatar presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Qatar, Sul piano militare e dual-use, Qatar mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Qatar, Legge 13/2016 sulla protezione dei dati e regimi QFC; quadro cyber centralizzato, con necessità di valutare accessi pubblici e legge applicabile. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Qatar, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,8/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,1	6,7	6,4	5,8	8,7	7,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,3	6,8	6,0	6,1	6,3	5,8

Il GCRI di Qatar è 7,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (6,8/10), mentre il più basso è Trasferibilità dati (5,8/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Qatar, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Qatar, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Qatar, Dal punto di vista italiano, Qatar rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Qatar è indicata una cooperazione selettiva, coerente con il FOTR di 6,2/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasferibilità dati a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

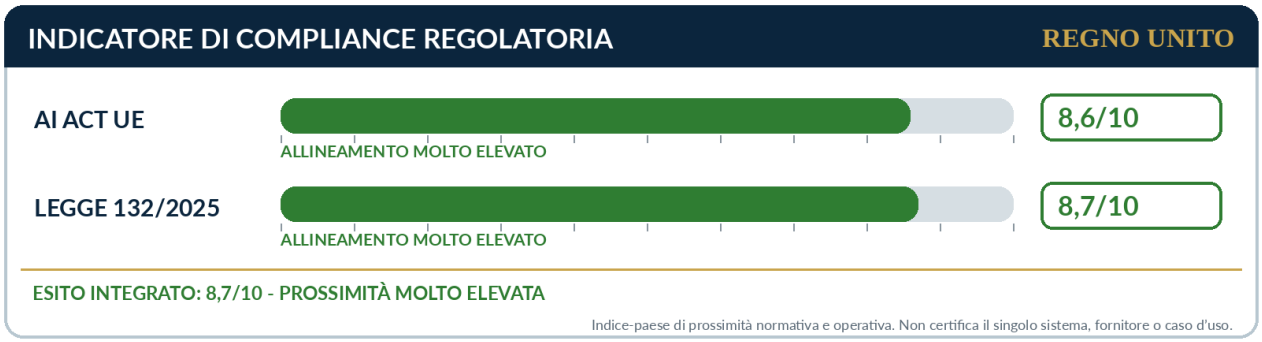
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Qatar: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Regno Unito

Posizione FOTR	22	Area	Europa	Subregione	Europa occidentale e centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	8,7	GCRI / 10	8,4	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Regno Unito, AI Act UE 8,6/10; legge 132/2025 8,7/10; esito integrato 8,7/10, classe «Allineamento molto elevato». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Regno Unito, situato in Europa occidentale e centrale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La partecipazione all'ecosistema Five Eyes rafforza l'integrazione informativa e tecnologica con il blocco anglosassone, ma rende necessario valutare i poteri di accesso extraterritoriale e la concentrazione cloud. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 92/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,4/10) e indice FOTR (8,7/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Regno Unito presenta un ecosistema digitale maturo, istituzioni generalmente prevedibili e una buona capacità di gestione degli incidenti. Il rischio residuo deriva soprattutto dalla concentrazione cloud, dalle dipendenze extraeuropee e dalla complessità delle filiere software.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	95,5% / 42,2 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 68.395 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	95,8 / 85,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	100,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	80,9/100 - rank 3	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	76/100 - Libero / Libero (92/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,0 / 7,6 / 5,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Regno Unito, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Regno Unito le evidenze principali sono GTMI 85,8/100, EGDI 95,8/100, GCI 100,0/100, AI readiness 80,9/100. La dimensione più robusta è maturità infrastrutturale (9,8/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,6/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Regno Unito è 9,8/10. La base statistica rileva utenti Internet pari al 95,5% nel 2024; 42,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 68.395 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Regno Unito al posto 3 con un valore medio di 80,9/100; il pilastro migliore è politiche pubbliche (100,0/100), quello più debole è sviluppo e diffusione (68,5/100). Il GTMI 2025 è 85,8/100. Il punteggio S2 è 8,3/10 e indica una capacità elevata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Regno Unito è valutata solida, con S3 pari a 8,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 94,5/100, sviluppo e diffusione dell'IA 68,5/100, penetrazione Internet 95,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Regno Unito ottiene S4 6,6/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Regno Unito, Fornitura prevalentemente nazionale, europea e statunitense, con catene hardware globali. In genere è possibile diversificare e imporre requisiti contrattuali elevati. L'impatto sulla valutazione è misurato da S4=6,6/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Regno Unito è S5 9,1/10. La base ITU registra ITU GCI 100,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure giuridiche (20,0/20). Freedom on the Net è 76/100 - Libero, mentre Freedom in the World è Libero (92/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: UK GDPR, Data Protection Act 2018, Investigatory Powers Act e NIS Regulations; adeguatezza UE soggetta a monitoraggio e quadro in evoluzione.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,0	Crimini finanziari	7,5
Reti criminali	7,0	Attori incorporati nello Stato	3,0
Attori stranieri	7,5	Attori del settore privato	7,5
Resilienza complessiva	7,6	Cooperazione internazionale	8,0
Politiche e norme nazionali	8,0	Forze dell'ordine	7,5
Antiriciclaggio	7,0	Prevenzione	8,0
Supporto vittime e testimoni	7,5	Rischio operativo FOTR-CY	5,6 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (7,0/10), criminalità finanziaria (7,5/10) e resilienza (7,6/10) colloca Regno Unito in una fascia di rischio significativo, pari a 5,6/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (7,5/10) e attori del settore privato (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Regno Unito assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Regno Unito, la resilienza complessiva è robusta (7,6/10); la cooperazione internazionale è robusta (8,0/10), le politiche e norme nazionali sono robuste (8,0/10) e la capacità delle forze dell'ordine è robusta (7,5/10). Completano il quadro antiriciclaggio 7,0/10, prevenzione 8,0/10 e supporto a vittime e testimoni 7,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Regno Unito, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Regno Unito. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Regno Unito, In Regno Unito le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La

disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Regno Unito, Il livello governativo di Regno Unito presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Regno Unito, Sul piano militare e dual-use, Regno Unito mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Regno Unito, UK GDPR, Data Protection Act 2018, Investigatory Powers Act e NIS Regulations; adeguatezza UE soggetta a monitoraggio e quadro in evoluzione. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Regno Unito, È disponibile una decisione UE di adeguatezza. L'operatore italiano deve comunque controllare la portata della decisione, i trasferimenti successivi, le misure di sicurezza e le eventuali discipline settoriali. La componente FOTR di trasferibilità è 9,1/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,8	8,3	8,4	6,6	9,1	8,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,5	9,9	6,9	9,9	8,3	9,1

Il GCRI di Regno Unito è 8,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Maturità cyber (9,9/10), mentre il più basso è Trasparenza istituzionale (6,9/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Basso	Medio-basso	Basso	Basso

La matrice applica il FOTR di 8,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Regno Unito, la cautela si concentra su 2 ambiti a rischio intermedio: Sanità e biometria, IP e R&S. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Regno Unito, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Regno Unito, Dal punto di vista italiano, Regno Unito rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Regno Unito, il FOTR di 8,7/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (6,9/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

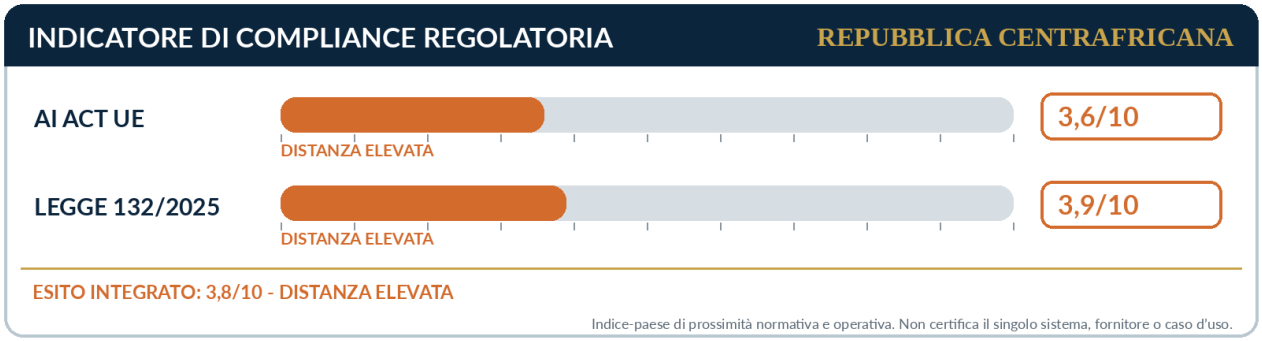
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Regno Unito: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Repubblica Centrafricana

Posizione FOTR	177	Area	Africa	Subregione	Africa centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	3,9	GCRI / 10	1,5	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Repubblica Centrafricana, AI Act UE 3,6/10; legge 132/2025 3,9/10; esito integrato 3,8/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Per un operatore italiano, Repubblica Centrafricana non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 5/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (3,9/10) supera il GCRI tecnico (1,5/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. In Repubblica Centrafricana la cooperazione tecnologica ordinaria deve essere limitata a progetti non critici, con isolamento, cifratura e supervisione italiana. Investimenti strategici necessitano di autorizzazioni e valutazioni rafforzate.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	13,8% / 0,0 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	18,2% / 2 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	9,5 / 18,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	4,8/100 - Tier 5 - capacità iniziali	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	11,9/100 - rank 192	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (5/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 2,1 / 6,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Repubblica Centrafricana, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Repubblica Centrafricana le evidenze principali sono GTMI 18,7/100, EGDI 9,5/100, GCI 4,8/100, AI readiness 11,9/100. La dimensione più robusta è indipendenza della supply chain (3,4/10), mentre la criticità relativa riguarda maturità infrastrutturale (0,2/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Repubblica Centrafricana è 0,2/10. La base statistica rileva utenti Internet pari al 13,8% nel 2024; 0,0 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 18,2% nel 2024; 2 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Repubblica Centrafricana al posto 192 con un valore medio di 11,9/100; il pilastro migliore è infrastrutture IA (22,6/100), quello più debole è governance (2,2/100). Il GTMI 2025 è 18,7/100. Il punteggio S2 è 1,4/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Repubblica Centrafricana è valutata fragile, con S3 pari a 1,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 17,1/100, sviluppo e diffusione dell'IA 9,6/100, penetrazione Internet 13,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Repubblica Centrafricana ottiene S4 3,4/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Repubblica Centrafricana, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è

sempre ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=3,4/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Repubblica Centrafricana è S5 0,7/10. La base ITU registra ITU GCI 4,8/100, Tier 5 - capacità iniziali; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (5/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	5,5
Reti criminali	8,0	Attori incorporati nello Stato	9,0
Attori stranieri	9,0	Attori del settore privato	6,5
Resilienza complessiva	2,1	Cooperazione internazionale	3,5
Politiche e norme nazionali	2,5	Forze dell'ordine	2,0
Antiriciclaggio	2,0	Prevenzione	2,0
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	6,5 - ALTO

Pressione del crimine digitale. Il profilo di Repubblica Centrafricana restituisce un rischio FOTR-CY di 6,5/10 (alto). La componente cyber-dipendente vale 3,0/10 e quella finanziaria 5,5/10; la risposta sistemica è valutata molto debole, con resilienza media di 2,1/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e attori stranieri (9,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Repubblica Centrafricana assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Repubblica Centrafricana, la resilienza complessiva è molto debole (2,1/10); la cooperazione internazionale è debole (3,5/10), le politiche e norme nazionali sono molto deboli (2,5/10) e la capacità delle forze dell'ordine è molto debole (2,0/10). Completano il quadro antiriciclaggio 2,0/10, prevenzione 2,0/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Repubblica Centrafricana, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Repubblica Centrafricana. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Repubblica Centrafricana, In Repubblica Centrafricana le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Repubblica Centrafricana, Il livello governativo di Repubblica Centrafricana presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Repubblica Centrafricana, Sul piano militare e dual-use, Repubblica Centrafricana mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Repubblica Centrafricana, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Repubblica Centrafricana, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 3,5/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
0,2	1,4	1,6	3,4	0,7	1,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,5	3,2	3,5	5,2	3,2	3,5

Il GCRI di Repubblica Centrafricana è 1,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 3,9/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,2/10), mentre il più basso è Maturità cyber (3,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Alto	Alto	Alto	Alto	Medio-alto

La matrice applica il FOTR di 3,9/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Repubblica Centrafricana, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Repubblica Centrafricana, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Repubblica Centrafricana, Dal punto di vista italiano, Repubblica Centrafricana rientra nella classe «Rischio alto»: cooperazione eccezionale e ad alto controllo, subordinata a assenza di dati

sensibili, verifica sanzionatoria, autorizzazioni interne e impossibilità di accesso ai sistemi strategici. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Repubblica Centrafricana ricade nella fascia di alto rischio (3,9/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

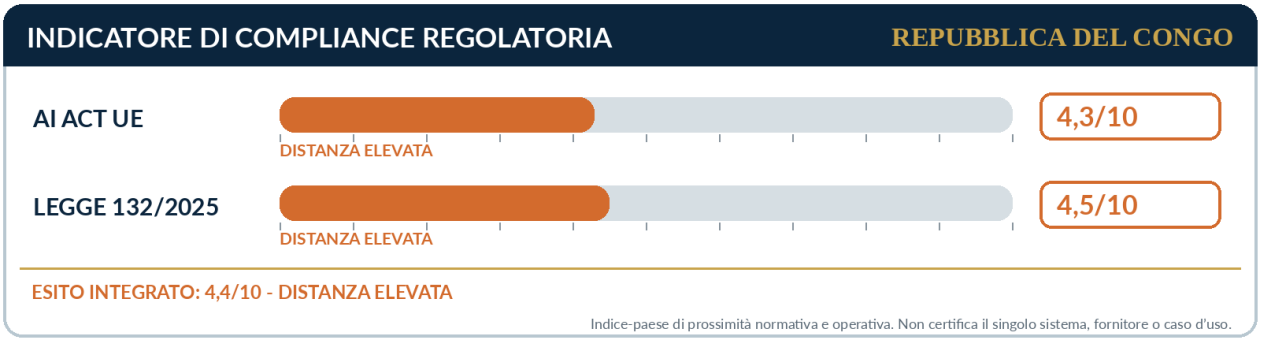
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Repubblica Centrafricana: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Repubblica del Congo

Posizione FOTR	151	Area	Africa	Subregione	Africa centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,5	GCRI / 10	3,4	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Repubblica del Congo, AI Act UE 4,3/10; legge 132/2025 4,5/10; esito integrato 4,4/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Repubblica del Congo è stato membro delle nazioni unite collocato in Africa centrale. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 17/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (4,5/10) supera il GCRI tecnico (3,4/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Per Repubblica del Congo non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	47,3% / 1,3 per 100	2024/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	53,0% / 17 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	33,9 / 16,5	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	27,6/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	26,5/100 - rank 144	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (17/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 3,1 / 5,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Repubblica del Congo, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Repubblica del Congo le evidenze principali sono GTMI 16,5/100, EGDI 33,9/100, GCI 27,6/100, AI readiness 26,5/100. La dimensione più robusta è capitale umano e competenze digitali (4,1/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,4/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Repubblica del Congo è 3,1/10. La base statistica rileva utenti Internet pari al 47,3% nel 2024; 1,3 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 53,0% nel 2024; 17 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Repubblica del Congo al posto 144 con un valore medio di 26,5/100; il pilastro migliore è governance (46,8/100), quello più debole è adozione pubblica (17,6/100). Il GTMI 2025 è 16,5/100. Il punteggio S2 è 2,4/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Repubblica del Congo è valutata fragile, con S3 pari a 4,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 46,4/100, sviluppo e diffusione dell'IA 23,4/100, penetrazione Internet 47,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Repubblica del Congo ottiene S4 4,1/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Repubblica del Congo, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre

ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Repubblica del Congo è S5 3,4/10. La base ITU registra ITU GCI 27,6/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (17/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	5,0
Reti criminali	6,5	Attori incorporati nello Stato	8,5
Attori stranieri	6,0	Attori del settore privato	4,0
Resilienza complessiva	3,1	Cooperazione internazionale	5,0
Politiche e norme nazionali	4,0	Forze dell'ordine	4,5
Antiriciclaggio	3,0	Prevenzione	3,5
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	5,2 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Repubblica del Congo presenta un'esposizione stimata significativa (5,2/10): reati cyber-dipendenti 2,0/10, crimini finanziari 5,0/10 e resilienza 3,1/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,5/10) e reti criminali (6,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Repubblica del Congo assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Repubblica del Congo, la resilienza complessiva è molto debole (3,1/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono deboli (4,0/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 3,0/10, prevenzione 3,5/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Repubblica del Congo, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Repubblica del Congo. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Repubblica del Congo, In Repubblica del Congo le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Repubblica del Congo, Il livello governativo di Repubblica del Congo presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Repubblica del Congo, Sul piano militare e dual-use, Repubblica del Congo mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Repubblica del Congo, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Repubblica del Congo, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,2/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,1	2,4	4,1	4,1	3,4	3,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,6	4,6	4,5	5,1	4,1	4,2

Il GCRI di Repubblica del Congo è 3,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,1/10), mentre il più basso è Supply chain (4,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Repubblica del Congo, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Repubblica del Congo, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Repubblica del Congo, Dal punto di vista italiano, Repubblica del Congo rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura

isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Repubblica del Congo ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

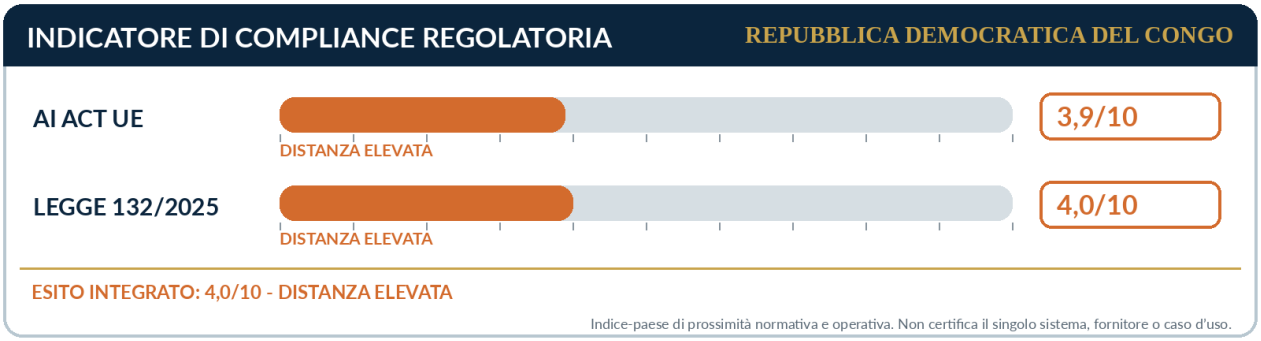
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Repubblica del Congo: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Repubblica Democratica del Congo

Posizione FOTR	175	Area	Africa	Subregione	Africa centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,0	GCRI / 10	3,1	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Repubblica Democratica del Congo, AI Act UE 3,9/10; legge 132/2025 4,0/10; esito integrato 4,0/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Repubblica Democratica del Congo presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 18/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (3,1/10) e indice FOTR (4,0/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Repubblica Democratica del Congo è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	19,7% / 0,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	22,5% / 10 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	27,1 / 39,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	56,6/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	26,5/100 - rank 144	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (18/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	1,5 / 2,2 / 6,3	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Repubblica Democratica del Congo, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Repubblica Democratica del Congo le evidenze principali sono GTMI 39,3/100, EGDI 27,1/100, GCI 56,6/100, AI readiness 26,5/100. La dimensione più robusta è postura di sicurezza cyber (4,1/10), mentre la criticità relativa riguarda maturità infrastrutturale (1,0/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Repubblica Democratica del Congo è 1,0/10. La base statistica rileva utenti Internet pari al 19,7% nel 2024; 0,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 22,5% nel 2024; 10 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Repubblica Democratica del Congo al posto 144 con un valore medio di 26,5/100; il pilastro migliore è governance (46,8/100), quello più debole è adozione pubblica (17,6/100). Il GTMI 2025 è 39,3/100. Il punteggio S2 è 2,8/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Repubblica Democratica del Congo è valutata fragile, con S3 pari a 3,9/10. Le evidenze disponibili comprendono indice UN di capitale umano 44,9/100, sviluppo e diffusione dell'IA 23,4/100, penetrazione Internet 19,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Repubblica Democratica del Congo ottiene S4 3,7/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Repubblica Democratica del Congo, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è

sempre ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=3,7/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Repubblica Democratica del Congo è S5 4,1/10. La base ITU registra ITU GCI 56,6/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (5,5/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (18/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	1,5	Crimini finanziari	8,0
Reti criminali	9,0	Attori incorporati nello Stato	9,0
Attori stranieri	9,0	Attori del settore privato	7,0
Resilienza complessiva	2,2	Cooperazione internazionale	3,5
Politiche e norme nazionali	3,0	Forze dell'ordine	1,5
Antiriciclaggio	1,5	Prevenzione	2,0
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	6,3 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Repubblica Democratica del Congo il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 6,3/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 1,5/10; le frodi e i reati finanziari 8,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (9,0/10) e attori incorporati nello Stato (9,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Repubblica Democratica del Congo assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Repubblica Democratica del Congo, la resilienza complessiva è molto debole (2,2/10); la cooperazione internazionale è debole (3,5/10), le politiche e norme nazionali sono molto deboli (3,0/10) e la capacità delle forze dell'ordine è molto debole (1,5/10). Completano il quadro antiriciclaggio 1,5/10, prevenzione 2,0/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Repubblica Democratica del Congo, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Repubblica Democratica del Congo. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Repubblica Democratica del Congo, In Repubblica Democratica del Congo le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Repubblica Democratica del Congo, Il livello governativo di Repubblica Democratica del Congo presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Repubblica Democratica del Congo, Sul piano militare e dual-use, Repubblica Democratica del Congo mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Repubblica Democratica del Congo, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Repubblica Democratica del Congo, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 3,3/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
1,0	2,8	3,9	3,7	4,1	3,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,8	3,5	3,7	4,9	3,2	3,3

Il GCRI di Repubblica Democratica del Congo è 3,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (4,9/10), mentre il più basso è Supply chain (3,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Alto	Medio-alto	Alto	Medio-alto

La matrice applica il FOTR di 4,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Repubblica Democratica del Congo, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Repubblica Democratica del Congo, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Repubblica Democratica del Congo, Dal punto di vista italiano, Repubblica Democratica del Congo rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici,

subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Repubblica Democratica del Congo ricade nella fascia di alto rischio (4,0/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

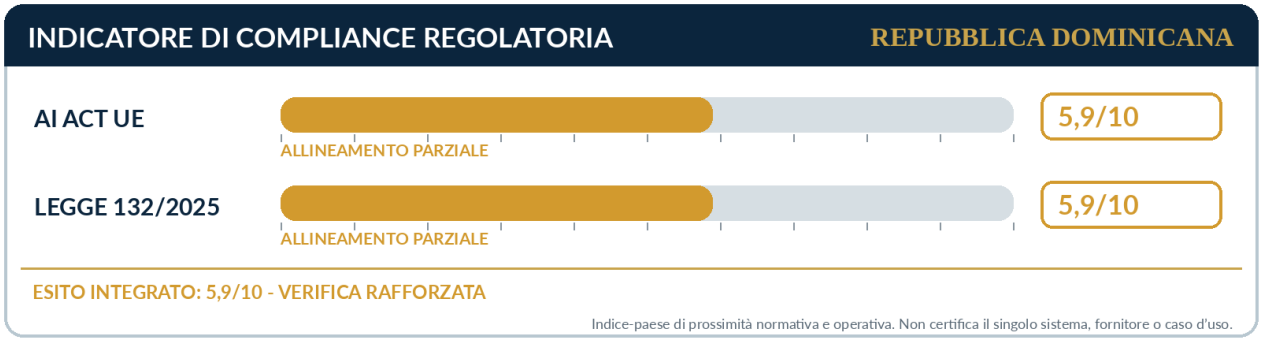
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Repubblica Democratica del Congo: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Repubblica Dominicana

Posizione FOTR	78	Area	Americhe	Subregione	Caraibi
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,9	GCRI / 10	6,1	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Repubblica Dominicana, AI Act UE 5,9/10; legge 132/2025 5,9/10; esito integrato 5,9/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Repubblica Dominicana, situato in Caraibi, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 67/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,1/10) e indice FOTR (5,9/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Repubblica Dominicana dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	91,0% / 11,2 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	99,5% / 181 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	70,1 / 82,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	75,7/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	47,6/100 - rank 84	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (67/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,0 / 4,9 / 4,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Repubblica Dominicana, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Repubblica Dominicana le evidenze principali sono GTMI 82,3/100, EGDI 70,1/100, GCI 75,7/100, AI readiness 47,6/100. La dimensione più robusta è maturità infrastrutturale (7,0/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,3/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Repubblica Dominicana è 7,0/10. La base statistica rileva utenti Internet pari al 91,0% nel 2024; 11,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 99,5% nel 2024; 181 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Repubblica Dominicana al posto 84 con un valore medio di 47,6/100; il pilastro migliore è adozione pubblica (70,6/100), quello più debole è sviluppo e diffusione (22,4/100). Il GTMI 2025 è 82,3/100. Il punteggio S2 è 5,5/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Repubblica Dominicana è valutata sufficiente ma disomogenea, con S3 pari a 5,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 71,9/100, sviluppo e diffusione dell'IA 22,4/100, penetrazione Internet 91,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Repubblica Dominicana ottiene S4 5,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Repubblica Dominicana, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software.

L'impatto sulla valutazione è misurato da S4=5,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Repubblica Dominicana è S5 7,0/10. La base ITU registra ITU GCI 75,7/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (10,6/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (67/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,0	Crimini finanziari	5,0
Reti criminali	5,5	Attori incorporati nello Stato	5,5
Attori stranieri	4,5	Attori del settore privato	4,5
Resilienza complessiva	4,9	Cooperazione internazionale	7,5
Politiche e norme nazionali	5,0	Forze dell'ordine	5,0
Antiriciclaggio	5,0	Prevenzione	5,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	4,8 - MODERATO

Pressione del crimine digitale. Il profilo di Repubblica Dominicana restituisce un rischio FOTR-CY di 4,8/10 (moderato). La componente cyber-dipendente vale 4,0/10 e quella finanziaria 5,0/10; la risposta sistemica è valutata debole, con resilienza media di 4,9/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (5,5/10) e attori incorporati nello Stato (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Repubblica Dominicana assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Repubblica Dominicana, la resilienza complessiva è debole (4,9/10); la cooperazione internazionale è robusta (7,5/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 5,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Repubblica Dominicana, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Repubblica Dominicana. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Repubblica Dominicana, In Repubblica Dominicana le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Repubblica Dominicana, Il livello governativo di Repubblica Dominicana presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Repubblica Dominicana, Sul piano militare e dual-use, Repubblica Dominicana mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Repubblica Dominicana, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Repubblica Dominicana, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,5/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,0	5,5	5,5	5,3	7,0	6,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,1	6,0	5,8	6,2	5,5	5,5

Il GCRI di Repubblica Dominicana è 6,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,9/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,2/10), mentre il più basso è Supply chain (5,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,9/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Repubblica Dominicana, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Repubblica Dominicana, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Repubblica Dominicana, Dal punto di vista italiano, Repubblica Dominicana rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Repubblica Dominicana è indicata una cooperazione selettiva, coerente con il FOTR di 5,9/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Supply chain a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

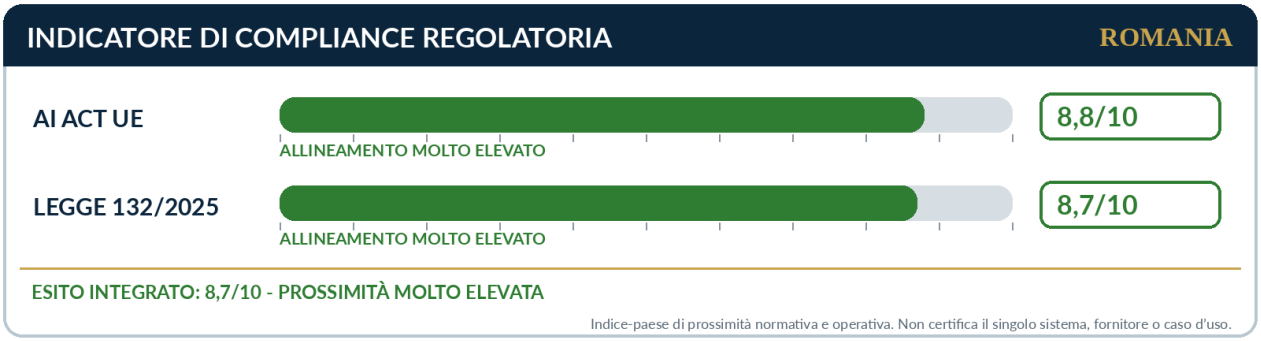
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Repubblica Dominicana: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Romania

Posizione FOTR	37	Area	Europa	Subregione	Europa sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,1	GCRI / 10	7,2	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Romania, AI Act UE 8,8/10; legge 132/2025 8,7/10; esito integrato 8,7/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Per un operatore italiano, Romania non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 83/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,2/10) e indice FOTR (8,1/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Romania offre condizioni favorevoli alla cooperazione tecnologica, con capacità istituzionali e cyber generalmente robuste. Restano differenze settoriali che rendono necessaria una verifica preventiva proporzionata ai dati e alla criticità del progetto.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	91,3% / 35,8 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 27.230 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	76,4 / 60,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	91,6/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	60,6/100 - rank 57	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (83/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,0 / 5,9 / 5,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Romania, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Romania le evidenze principali sono GTMI 60,2/100, EGDI 76,4/100, GCI 91,6/100, AI readiness 60,6/100. La dimensione più robusta è maturità infrastrutturale (9,1/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Romania è 9,1/10. La base statistica rileva utenti Internet pari al 91,3% nel 2024; 35,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 27.230 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Romania al posto 57 con un valore medio di 60,6/100; il pilastro migliore è politiche pubbliche (84,0/100), quello più debole è sviluppo e diffusione (38,1/100). Il GTMI 2025 è 60,2/100. Il punteggio S2 è 6,1/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Romania è valutata sufficiente ma disomogenea, con S3 pari a 6,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 74,4/100, sviluppo e diffusione dell'IA 38,1/100, penetrazione Internet 91,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Romania ottiene S4 5,9/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Romania, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=5,9/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Romania è S5 8,6/10. La base ITU registra ITU GCI 91,6/100, Tier 2 - avanzato; il pilastro relativamente più debole è misure tecniche (14,9/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (83/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, legge 190/2018 e disciplina nazionale di cybersicurezza/NIS2; quadro UE per AI, dati, piattaforme e prodotti digitali.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,0	Crimini finanziari	6,5
Reti criminali	5,5	Attori incorporati nello Stato	4,5
Attori stranieri	4,0	Attori del settore privato	4,0
Resilienza complessiva	5,9	Cooperazione internazionale	7,0
Politiche e norme nazionali	6,0	Forze dell'ordine	6,0
Antiriciclaggio	5,0	Prevenzione	6,0
Supporto vittime e testimoni	6,0	Rischio operativo FOTR-CY	5,2 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Romania restituisce un rischio FOTR-CY di 5,2/10 (significativo). La componente cyber-dipendente vale 6,0/10 e quella finanziaria 6,5/10; la risposta sistemica è valutata intermedia, con resilienza media di 5,9/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (5,5/10) e attori incorporati nello Stato (4,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Romania assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Romania, la resilienza complessiva è intermedia (5,9/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è intermedia (6,0/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 6,0/10 e supporto a vittime e testimoni 6,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Romania, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Romania. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Romania, In Romania le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Romania, Il livello governativo di Romania presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Romania, Sul piano militare e dual-use, Romania mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Romania, GDPR, legge 190/2018 e disciplina nazionale di cybersicurezza/NIS2; quadro UE per AI, dati, piattaforme e prodotti digitali. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Romania, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 8,9/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,1	6,1	6,5	5,9	8,6	7,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,5	7,7	7,5	8,4	7,2	8,9

Il GCRI di Romania è 7,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,1/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (8,9/10), mentre il più basso è Supply chain (7,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,1/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Romania, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Romania, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Romania, Dal punto di vista italiano, Romania rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Romania, il FOTR di 8,1/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (7,2/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

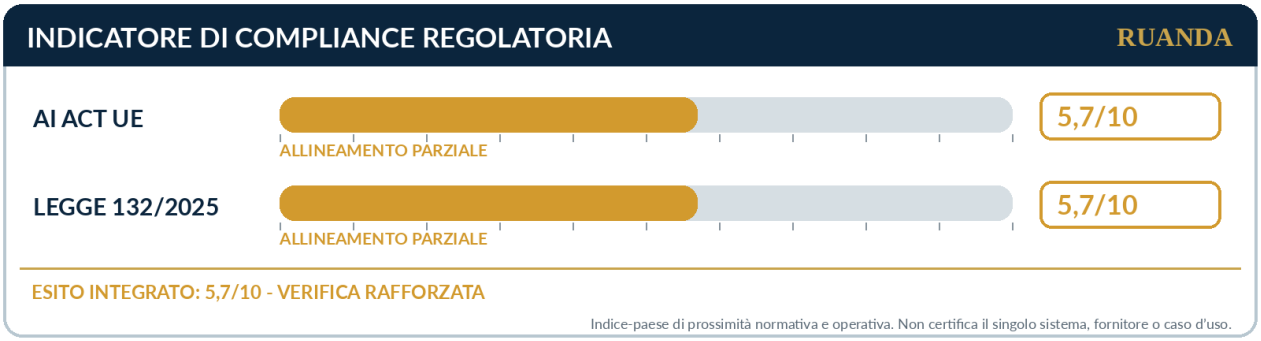
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Romania: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Ruanda

Posizione FOTR	102	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,7	GCRI / 10	5,4	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Ruanda, AI Act UE 5,7/10; legge 132/2025 5,7/10; esito integrato 5,7/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Ruanda è stato membro delle nazioni unite collocato in Africa orientale. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 21/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,4/10) e indice FOTR (5,7/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il quadro di Ruanda è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	31,7% / 0,6 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	72,0% / 161 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	58,0 / 82,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	98,1/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	54,0/100 - rank 74	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	34/100 - Non libero / Non libero (21/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 5,0 / 4,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Ruanda, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Ruanda le evidenze principali sono GTMI 82,9/100, EGDI 58,0/100, GCI 98,1/100, AI readiness 54,0/100. La dimensione più robusta è postura di sicurezza cyber (7,2/10), mentre la criticità relativa riguarda maturità infrastrutturale (3,4/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Ruanda è 3,4/10. La base statistica rileva utenti Internet pari al 31,7% nel 2024; 0,6 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 72,0% nel 2024; 161 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Ruanda al posto 74 con un valore medio di 54,0/100; il pilastro migliore è governance (78,8/100), quello più debole è sviluppo e diffusione (29,4/100). Il GTMI 2025 è 82,9/100. Il punteggio S2 è 6,1/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Ruanda è valutata sufficiente ma disomogenea, con S3 pari a 5,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 54,7/100, sviluppo e diffusione dell'IA 29,4/100, penetrazione Internet 31,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Ruanda ottiene S4 5,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Ruanda, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=5,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Ruanda è S5 7,2/10. La base ITU registra ITU GCI 98,1/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure tecniche (19,0/20). Freedom on the Net è 34/100 - Non libero, mentre Freedom in the World è Non libero (21/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge 058/2021 sulla protezione dei dati e quadro cyber centralizzato; buona capacità progettuale, con attenzione agli accessi pubblici.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	6,5
Reti criminali	3,0	Attori incorporati nello Stato	6,0
Attori stranieri	4,0	Attori del settore privato	3,0
Resilienza complessiva	5,0	Cooperazione internazionale	5,0
Politiche e norme nazionali	6,0	Forze dell'ordine	5,5
Antiriciclaggio	5,5	Prevenzione	5,5
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	4,9 - MODERATO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (4,5/10), criminalità finanziaria (6,5/10) e resilienza (5,0/10) colloca Ruanda in una fascia di rischio moderato, pari a 4,9/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (6,0/10) e attori stranieri (4,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Ruanda assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Ruanda, la resilienza complessiva è debole (5,0/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 5,5/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Ruanda, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Ruanda. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Ruanda, In Ruanda le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Ruanda, Il livello governativo di Ruanda presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Ruanda, Sul piano militare e dual-use, Ruanda mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Ruanda, Legge 058/2021 sulla protezione dei dati e quadro cyber centralizzato; buona capacità progettuale, con attenzione agli accessi pubblici. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Ruanda, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,4/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,4	6,1	5,2	5,3	7,2	5,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,7	5,9	5,3	6,2	5,6	5,4

Il GCRI di Ruanda è 5,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,2/10), mentre il più basso è Trasparenza istituzionale (5,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Ruanda, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Ruanda, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Ruanda, Dal punto di vista italiano, Ruanda rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Ruanda è indicata una cooperazione selettiva, coerente con il FOTR di 5,7/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasparenza istituzionale a decisione caso per caso.

Presidi minimi raccomandati

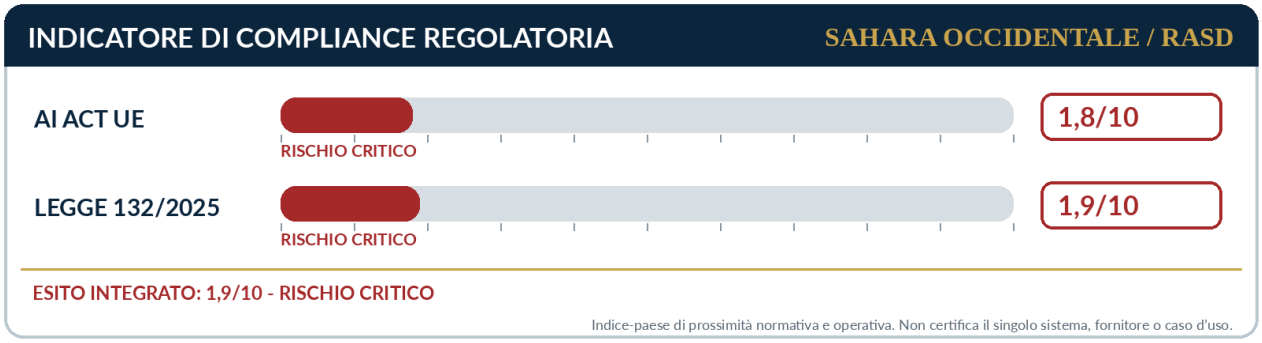
Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Ruanda: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Sahara Occidentale / RASD

Posizione FOTR	193	Area	Africa	Subregione	Sahara occidentale
Status	Territorio conteso; inclusione a fini esclusivamente analitici	Confidenza Celeborn Intelligence	Bassa	Copertura dati	0/7 famiglie
FOTR / 10	1,8	GCRI / 10	1,9	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Sahara Occidentale / RASD, AI Act UE 1,8/10; legge 132/2025 1,9/10; esito integrato 1,9/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Sahara Occidentale / RASD presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 4/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (1,9/10) e indice FOTR (1,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Territorio conteso, con amministrazioni e infrastrutture non uniformi; l'assenza di un quadro univoco rende i progetti digitali altamente complessi.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	n.d. / n.d. per 100	n.d./n.d.	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	n.d. / n.d. per milione	n.d./n.d.	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	n.d. / n.d.	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	n.d./100 - n.d.	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	n.d./100 - rank n.d.	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (4/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,2 / 4,4 / 6,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Sahara Occidentale / RASD, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 0/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Sahara Occidentale / RASD le evidenze principali sono nessun indicatore composito pienamente comparabile. La dimensione più robusta è indipendenza della supply chain (3,7/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (1,2/10). Sono disponibili 0 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata bassa. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Sahara Occidentale / RASD è 1,5/10. La base statistica rileva i principali dati WDI non sono disponibili in forma omogenea. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Per Sahara Occidentale / RASD non è disponibile un profilo Oxford Insights direttamente attribuibile; l'adozione di IA è quindi valutata attraverso GovTech, servizi online, infrastrutture e fonti qualitative. Il punteggio S2 è 1,6/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Sahara Occidentale / RASD è valutata fragile, con S3 pari a 1,2/10. Le evidenze disponibili comprendono evidenza quantitativa incompleta. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Sahara Occidentale / RASD ottiene S4 3,7/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Sahara Occidentale / RASD, Fornitura non uniforme, dipendente dall'amministrazione effettiva del territorio e da reti marocchine o locali. L'impatto sulla valutazione è misurato da S4=3,7/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Sahara Occidentale / RASD è S5 1,3/10. La base ITU registra GCI non disponibile in forma comparabile. Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (4/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,2	Crimini finanziari	7,6
Reti criminali	6,0	Attori incorporati nello Stato	7,4
Attori stranieri	5,2	Attori del settore privato	4,4
Resilienza complessiva	4,4	Cooperazione internazionale	5,4
Politiche e norme nazionali	6,2	Forze dell'ordine	5,5
Antiriciclaggio	4,0	Prevenzione	3,7
Supporto vittime e testimoni	3,7	Rischio operativo FOTR-CY	6,0 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Sahara Occidentale / RASD presenta un'esposizione stimata significativa (6,0/10): reati cyber-dipendenti 4,2/10, crimini finanziari 7,6/10 e resilienza 4,4/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,4/10) e reti criminali (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Sahara Occidentale / RASD assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Sahara Occidentale / RASD, la resilienza complessiva è debole (4,4/10); la cooperazione internazionale è debole (5,4/10), le politiche e norme nazionali sono intermedie (6,2/10) e la capacità delle forze dell'ordine è debole (5,5/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 3,7/10 e supporto a vittime e testimoni 3,7/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Sahara Occidentale / RASD, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE. Poiché l'entità non dispone di una serie nazionale GI-TOC autonoma, i valori derivano da un proxy Celeborn Intelligence ponderato su Marocco 50%, Algeria 40%, Mauritania 10%; la confidenza deve pertanto essere considerata inferiore e la decisione resa più prudente.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; proxy Celeborn Intelligence ponderato su Marocco 50%, Algeria 40%, Mauritania 10%. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Sahara Occidentale / RASD, In Sahara Occidentale / RASD le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Sahara Occidentale / RASD, Il livello governativo di Sahara Occidentale / RASD presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Sahara Occidentale / RASD, Sul piano militare e dual-use, Sahara Occidentale / RASD mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Sahara Occidentale / RASD, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Sahara Occidentale / RASD, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 1,3/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
1,5	1,6	1,2	3,7	1,3	1,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
2,6	1,3	1,2	3,0	1,4	1,3

Il GCRI di Sahara Occidentale / RASD è 1,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 1,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (3,0/10), mentre il più basso è Trasparenza istituzionale (1,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 1,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Sahara Occidentale / RASD, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Sahara Occidentale / RASD, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Sahara Occidentale / RASD, Dal punto di vista italiano, Sahara Occidentale / RASD rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie,

subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Sahara Occidentale / RASD, il FOTR di 1,8/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

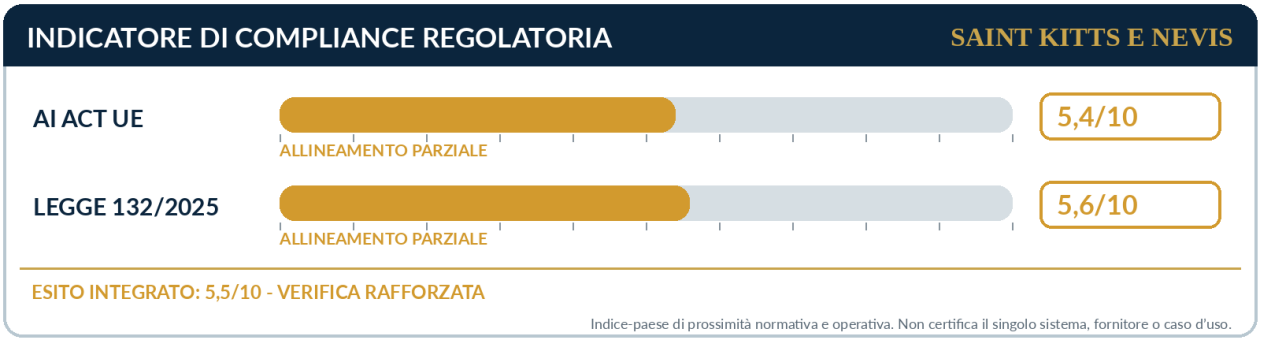
Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.
Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.
Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Sahara Occidentale / RASD: World Development Indicators, valori più recenti disponibili 2022-2024; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Bassa con copertura 0/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Saint Kitts e Nevis

Posizione FOTR	103	Area	Americhe	Subregione	Caraibi
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,7	GCRI / 10	5,0	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Saint Kitts e Nevis, AI Act UE 5,4/10; legge 132/2025 5,6/10; esito integrato 5,5/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Saint Kitts e Nevis, situato in Caraibi, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 89/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,0/10) e indice FOTR (5,7/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Saint Kitts e Nevis dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	76,9% / 46,7 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 11.720 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	63,1 / 28,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	31,6/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	20,2/100 - rank 170	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (89/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	1,5 / 5,4 / 3,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Saint Kitts e Nevis, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Saint Kitts e Nevis le evidenze principali sono GTMI 28,8/100, EGDI 63,1/100, GCI 31,6/100, AI readiness 20,2/100. La dimensione più robusta è maturità infrastrutturale (8,8/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,4/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Saint Kitts e Nevis è 8,8/10. La base statistica rileva utenti Internet pari al 76,9% nel 2024; 46,7 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 100,0% nel 2024; 11.720 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Saint Kitts e Nevis al posto 170 con un valore medio di 20,2/100; il pilastro migliore è infrastrutture IA (33,7/100), quello più debole è adozione pubblica (5,4/100). Il GTMI 2025 è 28,8/100. Il punteggio S2 è 2,4/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Saint Kitts e Nevis è valutata sufficiente ma disomogenea, con S3 pari a 5,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 72,0/100, sviluppo e diffusione dell'IA 12,8/100, penetrazione Internet 76,9%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Saint Kitts e Nevis ottiene S4 4,7/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Saint Kitts e Nevis, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto

sulla valutazione è misurato da S4=4,7/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Saint Kitts e Nevis è S5 4,1/10. La base ITU registra ITU GCI 31,6/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (1,8/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (89/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	1,5	Crimini finanziari	4,5
Reti criminali	5,0	Attori incorporati nello Stato	5,0
Attori stranieri	5,5	Attori del settore privato	1,5
Resilienza complessiva	5,4	Cooperazione internazionale	6,0
Politiche e norme nazionali	6,5	Forze dell'ordine	5,0
Antiriciclaggio	6,0	Prevenzione	4,5
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	3,8 - MODERATO

Sintesi del rischio cybercrime. Saint Kitts e Nevis presenta un'esposizione stimata moderata (3,8/10): reati cyber-dipendenti 1,5/10, crimini finanziari 4,5/10 e resilienza 5,4/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (5,5/10) e reti criminali (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Saint Kitts e Nevis assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Saint Kitts e Nevis, la resilienza complessiva è debole (5,4/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 4,5/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Saint Kitts e Nevis, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Saint Kitts e Nevis. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Saint Kitts e Nevis, In Saint Kitts e Nevis le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Saint Kitts e Nevis, Il livello governativo di Saint Kitts e Nevis presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Saint Kitts e Nevis, Sul piano militare e dual-use, Saint Kitts e Nevis mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Saint Kitts e Nevis, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Saint Kitts e Nevis, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,3/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,8	2,4	5,0	4,7	4,1	5,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,7	5,5	6,1	6,2	5,3	5,3

Il GCRI di Saint Kitts e Nevis è 5,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,2/10), mentre il più basso è Supply chain (5,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Saint Kitts e Nevis, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Saint Kitts e Nevis, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Saint Kitts e Nevis, Dal punto di vista italiano, Saint Kitts e Nevis rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Saint Kitts e Nevis è indicata una cooperazione selettiva, coerente con il FOTR di 5,7/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Supply chain a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

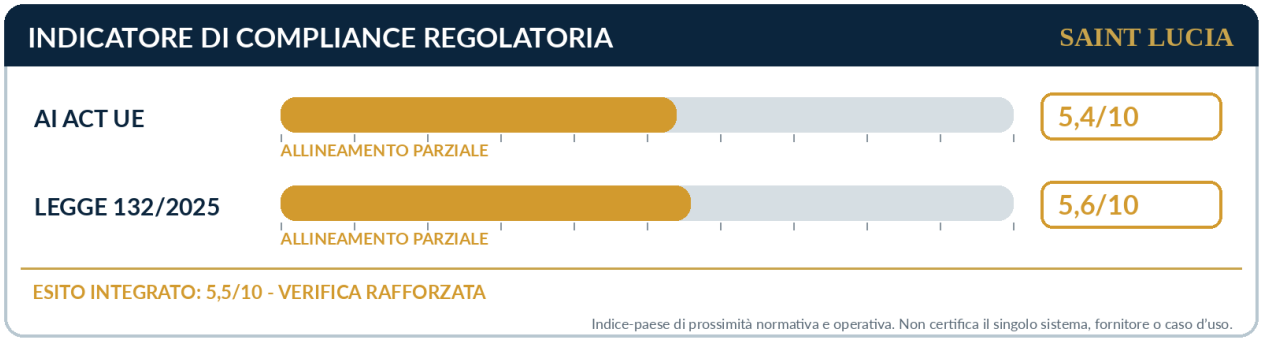
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Saint Kitts e Nevis: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Saint Lucia

Posizione FOTR	110	Area	Americhe	Subregione	Caraibi
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,6	GCRI / 10	4,3	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Saint Lucia, AI Act UE 5,4/10; legge 132/2025 5,6/10; esito integrato 5,5/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Saint Lucia non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 91/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,6/10) supera il GCRI tecnico (4,3/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. In Saint Lucia la trasformazione digitale procede più rapidamente dell'uniformità regolatoria e operativa. Gli investimenti devono essere accompagnati da audit, clausole di uscita e gestione locale del rischio.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	68,2% / 13,6 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 734 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	52,5 / 35,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	26,2/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	25,2/100 - rank 142	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (91/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 5,5 / 3,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Saint Lucia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Saint Lucia le evidenze principali sono GTMI 35,3/100, EGDI 52,5/100, GCI 26,2/100, AI readiness 25,2/100. La dimensione più robusta è maturità infrastrutturale (6,3/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,0/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Saint Lucia è 6,3/10. La base statistica rileva utenti Internet pari al 68,2% nel 2024; 13,6 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 100,0% nel 2024; 734 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Saint Lucia al posto 142 con un valore medio di 25,2/100; il pilastro migliore è infrastrutture IA (40,2/100), quello più debole è politiche pubbliche (4,0/100). Il GTMI 2025 è 35,3/100. Il punteggio S2 è 3,0/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Saint Lucia è valutata fragile, con S3 pari a 4,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 60,4/100, sviluppo e diffusione dell'IA 13,0/100, penetrazione Internet 68,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Saint Lucia ottiene S4 4,2/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Saint Lucia, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=4,2/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Saint Lucia è S5 3,6/10. La base ITU registra ITU GCI 26,2/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (91/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	2,5
Reti criminali	4,5	Attori incorporati nello Stato	3,0
Attori stranieri	6,0	Attori del settore privato	1,5
Resilienza complessiva	5,5	Cooperazione internazionale	6,0
Politiche e norme nazionali	6,5	Forze dell'ordine	4,5
Antiriciclaggio	4,5	Prevenzione	6,0
Supporto vittime e testimoni	5,5	Rischio operativo FOTR-CY	3,4 - MODERATO

Rischio criminale connesso alle tecnologie. In Saint Lucia il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 3,4/10, livello moderato. I reati che dipendono direttamente da sistemi informatici raggiungono 2,0/10; le frodi e i reati finanziari 2,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (6,0/10) e reti criminali (4,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Saint Lucia assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Saint Lucia, la resilienza complessiva è intermedia (5,5/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 5,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Saint Lucia, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Saint Lucia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Saint Lucia, In Saint Lucia le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Saint Lucia, Il livello governativo di Saint Lucia presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Saint Lucia, Sul piano militare e dual-use, Saint Lucia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Saint Lucia, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Saint Lucia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,5/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,3	3,0	4,5	4,2	3,6	4,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,9	5,2	5,8	6,1	5,2	5,5

Il GCRI di Saint Lucia è 4,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,1/10), mentre il più basso è Maturità cyber (5,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio-alto	Medio	Medio	Medio

La matrice applica il FOTR di 5,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Saint Lucia, 1 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Cloud e infrastrutture. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Saint Lucia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Saint Lucia, Dal punto di vista italiano, Saint Lucia rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Saint Lucia è indicata una cooperazione selettiva, coerente con il FOTR di 5,6/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Cloud e infrastrutture a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

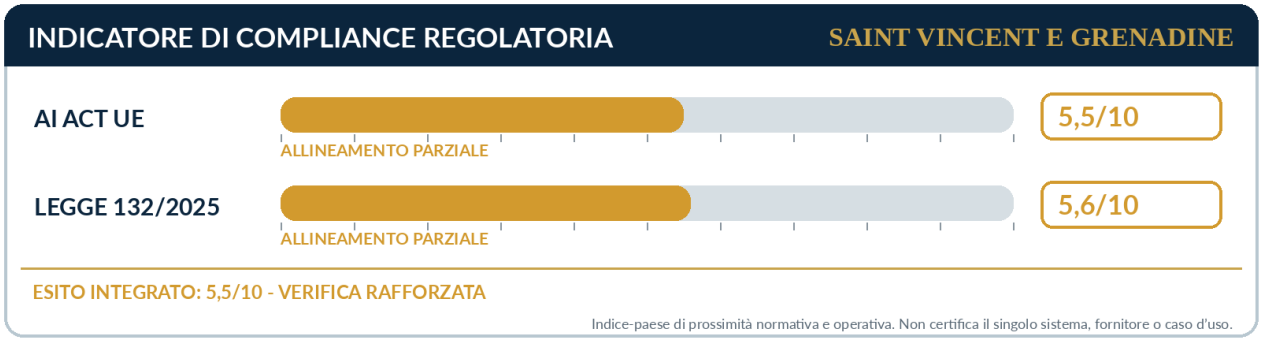
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Saint Lucia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Saint Vincent e Grenadine

Posizione FOTR	104	Area	Americhe	Subregione	Caraibi
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,7	GCRI / 10	4,5	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Saint Vincent e Grenadine, AI Act UE 5,5/10; legge 132/2025 5,6/10; esito integrato 5,5/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Saint Vincent e Grenadine è stato membro delle nazioni unite collocato in Caraibi. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 90/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,7/10) supera il GCRI tecnico (4,5/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Saint Vincent e Grenadine dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	76,2% / 29,5 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 268 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	58,8 / 33,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	26,5/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	20,9/100 - rank 166	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (90/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 5,4 / 3,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Saint Vincent e Grenadine, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Saint Vincent e Grenadine le evidenze principali sono GTMI 33,9/100, EGDI 58,8/100, GCI 26,5/100, AI readiness 20,9/100. La dimensione più robusta è maturità infrastrutturale (7,2/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,7/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Saint Vincent e Grenadine è 7,2/10. La base statistica rileva utenti Internet pari al 76,2% nel 2024; 29,5 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 268 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Saint Vincent e Grenadine al posto 166 con un valore medio di 20,9/100; il pilastro migliore è infrastrutture IA (32,6/100), quello più debole è politiche pubbliche (11,5/100). Il GTMI 2025 è 33,9/100. Il punteggio S2 è 2,7/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Saint Vincent e Grenadine è valutata fragile, con S3 pari a 4,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 69,6/100, sviluppo e diffusione dell'IA 13,0/100, penetrazione Internet 76,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Saint Vincent e Grenadine ottiene S4 4,3/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Saint Vincent e Grenadine, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software.

L'impatto sulla valutazione è misurato da S4=4,3/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Saint Vincent e Grenadine è S5 3,6/10. La base ITU registra ITU GCI 26,5/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (90/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	2,5
Reti criminali	5,0	Attori incorporati nello Stato	2,0
Attori stranieri	5,5	Attori del settore privato	2,0
Resilienza complessiva	5,4	Cooperazione internazionale	6,0
Politiche e norme nazionali	6,5	Forze dell'ordine	4,5
Antiriciclaggio	5,5	Prevenzione	5,5
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	3,7 - MODERATO

Sintesi del rischio cybercrime. Saint Vincent e Grenadine presenta un'esposizione stimata moderata (3,7/10): reati cyber-dipendenti 3,0/10, crimini finanziari 2,5/10 e resilienza 5,4/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (5,5/10) e reti criminali (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Saint Vincent e Grenadine assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Saint Vincent e Grenadine, la resilienza complessiva è debole (5,4/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 5,5/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Saint Vincent e Grenadine, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Saint Vincent e Grenadine. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Saint Vincent e Grenadine, In Saint Vincent e Grenadine le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Saint Vincent e Grenadine, Il livello governativo di Saint Vincent e Grenadine presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Saint Vincent e Grenadine, Sul piano militare e dual-use, Saint Vincent e Grenadine mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Saint Vincent e Grenadine, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Saint Vincent e Grenadine, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,8/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,2	2,7	4,6	4,3	3,6	4,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,2	5,2	5,7	5,9	5,2	5,8

Il GCRI di Saint Vincent e Grenadine è 4,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (6,2/10), mentre il più basso è Maturità cyber (5,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio-alto	Medio	Medio	Medio

La matrice applica il FOTR di 5,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Saint Vincent e Grenadine, 1 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Cloud e infrastrutture. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Saint Vincent e Grenadine, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Saint Vincent e Grenadine, Dal punto di vista italiano, Saint Vincent e Grenadine rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Saint Vincent e Grenadine è indicata una cooperazione selettiva, coerente con il FOTR di 5,7/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Cloud e infrastrutture a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

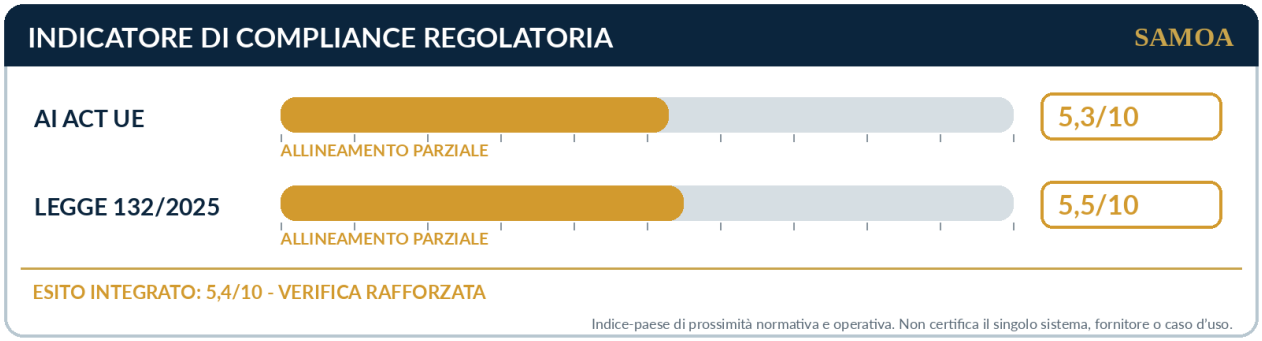
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Saint Vincent e Grenadine: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Samoa

Posizione FOTR	111	Area	Oceania	Subregione	Pacifico insulare
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,6	GCRI / 10	4,0	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Samoa, AI Act UE 5,3/10; legge 132/2025 5,5/10; esito integrato 5,4/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Oceania, Samoa presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La distanza geografica e l'insularità rendono centrali cavi sottomarini, satelliti, continuità energetica e dipendenza da fornitori australiani, neozelandesi, statunitensi o asiatici. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 84/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,6/10) supera il GCRI tecnico (4,0/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il quadro di Samoa è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	21,2% / 0,9 per 100	2014/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 605 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	49,0 / 35,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	43,1/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	22,5/100 - rank 154	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (84/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 5,9 / 3,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Samoa, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Samoa le evidenze principali sono GTMI 35,2/100, EGDI 49,0/100, GCI 43,1/100, AI readiness 22,5/100. La dimensione più robusta è postura di sicurezza cyber (4,6/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,8/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Samoa è 4,0/10. La base statistica rileva utenti Internet pari al 21,2% nel 2014; 0,9 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 100,0% nel 2024; 605 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Samoa al posto 154 con un valore medio di 22,5/100; il pilastro migliore è resilienza (41,3/100), quello più debole è politiche pubbliche (4,0/100). Il GTMI 2025 è 35,2/100. Il punteggio S2 è 2,8/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Samoa è valutata fragile, con S3 pari a 4,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 64,5/100, sviluppo e diffusione dell'IA 17,5/100, penetrazione Internet 21,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Samoa ottiene S4 4,2/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Samoa, Dipendenza da Australia, Nuova Zelanda, Stati Uniti, Francia e operatori satellitari o sottomarini; la scala ridotta limita la diversificazione e aumenta il rischio di concentrazione. L'impatto sulla

valutazione è misurato da S4=4,2/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Samoa è S5 4,6/10. La base ITU registra ITU GCI 43,1/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (4,6/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (84/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	3,5
Reti criminali	3,0	Attori incorporati nello Stato	2,5
Attori stranieri	3,5	Attori del settore privato	1,0
Resilienza complessiva	5,9	Cooperazione internazionale	6,0
Politiche e norme nazionali	6,5	Forze dell'ordine	6,5
Antiriciclaggio	5,5	Prevenzione	6,5
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	3,4 - MODERATO

Quadro criminale digitale. Per Samoa, l'indice operativo FOTR-CY è 3,4/10, classe moderata. Il mercato dei reati cyber-dipendenti è limitato o poco osservabile (3,0/10), mentre i crimini finanziari sono intermedi (3,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (3,5/10) e reti criminali (3,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Samoa assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Samoa, la resilienza complessiva è intermedia (5,9/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è intermedia (6,5/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 6,5/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Samoa, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Samoa. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Samoa, In Samoa le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Samoa, Il livello governativo di Samoa presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il

settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Samoa, Sul piano militare e dual-use, Samoa mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Samoa, Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Samoa, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,1/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
4,0	2,8	4,4	4,2	4,6	4,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,9	4,9	5,8	6,8	4,5	5,1

Il GCRI di Samoa è 4,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,8/10), mentre il più basso è Supply chain (4,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio-alto	Medio	Medio	Medio

La matrice applica il FOTR di 5,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Samoa, 1 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Cloud e infrastrutture. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Samoa, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Samoa, Dal punto di vista italiano, Samoa rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Samoa è indicata una cooperazione selettiva, coerente con il FOTR di 5,6/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Cloud e infrastrutture a decisione caso per caso.

Presidi minimi raccomandati

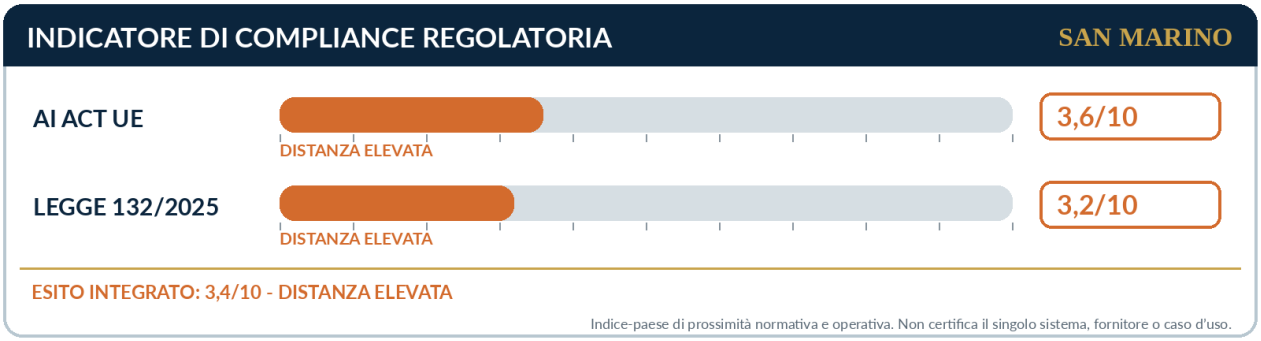
Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Samoa: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

San Marino

Posizione FOTR	182	Area	Europa	Subregione	Europa meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	3,8	GCRI / 10	4,2	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di San Marino, AI Act UE 3,6/10; legge 132/2025 3,2/10; esito integrato 3,4/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

San Marino occupa una posizione peculiare: è uno Stato sovrano completamente circondato dall'Italia, fortemente connesso all'economia e alle reti italiane, ma esterno all'Unione europea e allo Spazio economico europeo. Nel 2026 l'accordo quadro triennale con BYD ha indicato il territorio sammarinese come ambiente reale di sperimentazione per mobilità, accumulo, fotovoltaico, ricarica ultra-veloce, omologazione e valorizzazione di brevetti; la successiva missione istituzionale a Shenzhen ha inoltre collegato tale traiettoria a robotica, intelligenza artificiale, energia e infrastrutture. L'Atlante non considera la cooperazione con la Cina un rischio automatico, ma valuta la combinazione tra concentrazione del fornitore, integrazione di sistemi fisici e digitali, manutenzione remota, assenza di adeguatezza UE e limitata scala regolatoria. Da questa combinazione deriva la valutazione prudenziale di 3,8/10. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 97/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (4,2/10) e indice FOTR (3,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. La vicinanza territoriale e l'intensità dei rapporti con l'Italia non eliminano i rischi derivanti dalla limitata scala regolatoria, dall'assenza di adeguatezza UE e dalla crescente concentrazione di progetti energetici e tecnologici integrati con un grande fornitore cinese. L'Atlante adotta pertanto una valutazione prudenziale inferiore a 4/10.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	97,4% / 35,8 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 36.024 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	65,5 / 22,5	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	25,9/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	35,4/100 - rank 112	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (97/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	1,5 / 5,3 / 4,3	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di San Marino, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per San Marino le evidenze principali sono GTMI 22,5/100, EGDI 65,5/100, GCI 25,9/100, AI readiness 35,4/100. La dimensione più robusta è maturità infrastrutturale (7,0/10), mentre la criticità relativa riguarda indipendenza della supply chain (2,2/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di San Marino è 7,0/10. La base statistica rileva utenti Internet pari al 97,4% nel 2024; 35,8 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 100,0% nel 2024; 36.024 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca San Marino al posto 112 con un valore medio di 35,4/100; il pilastro migliore è governance (45,6/100), quello più debole è adozione pubblica (23,9/100). Il GTMI 2025 è 22,5/100. Il punteggio S2 è 4,2/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di San Marino è valutata fragile, con S3 pari a 4,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 65,9/100, sviluppo e diffusione dell'IA 33,3/100, penetrazione Internet 97,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di San Marino ottiene S4 2,2/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/Unione europea, Stati Uniti e Cina; l'indicatore di indipendenza disponibile è 2,5/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository,

chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di San Marino, Dipendenza strutturale dall'ecosistema italiano ed europeo, oggi affiancata da una cooperazione strategica con il gruppo cinese BYD su mobilità, accumulo energetico, fotovoltaico, infrastrutture di ricarica, sandbox regolamentare e valorizzazione della proprietà intellettuale. L'impatto sulla valutazione è misurato da S4=2,2/10 e dal proxy di indipendenza 2,5/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di San Marino è S5 2,9/10. La base ITU registra ITU GCI 25,9/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (97/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Disciplina nazionale della protezione dei dati, delle comunicazioni elettroniche e dei reati informatici, con differenze rispetto al GDPR; trasferimenti e accessi pubblici richiedono una verifica locale aggiornata.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	1,5	Crimini finanziari	7,0
Reti criminali	3,0	Attori incorporati nello Stato	5,0
Attori stranieri	6,5	Attori del settore privato	5,5
Resilienza complessiva	5,3	Cooperazione internazionale	6,0
Politiche e norme nazionali	5,5	Forze dell'ordine	5,0
Antiriciclaggio	4,5	Prevenzione	4,5
Supporto vittime e testimoni	5,5	Rischio operativo FOTR-CY	4,3 - MODERATO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (1,5/10), criminalità finanziaria (7,0/10) e resilienza (5,3/10) colloca San Marino in una fascia di rischio moderato, pari a 4,3/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (6,5/10) e attori del settore privato (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di San Marino assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di San Marino, la resilienza complessiva è debole (5,3/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 4,5/10 e supporto a vittime e testimoni 5,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in San Marino, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di San Marino. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per San Marino, In San Marino le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per San Marino, Il livello governativo di San Marino presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per San Marino, Sul piano militare e dual-use, San Marino mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per San Marino, Disciplina nazionale della protezione dei dati, delle comunicazioni elettroniche e dei reati informatici, con differenze rispetto al GDPR; trasferimenti e accessi pubblici richiedono una verifica locale aggiornata. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso San Marino, San Marino non appartiene al SEE e non beneficia di una decisione generale di adeguatezza UE. I flussi dall'Italia richiedono quindi uno specifico fondamento del capo V GDPR, TIA e misure supplementari. La prevista integrazione di piattaforme energetiche e infrastrutturali con un fornitore cinese aumenta la necessità di separare telemetria, manutenzione remota, identità, log, chiavi e dati dei cittadini. La componente FOTR di trasferibilità è 3,6/10 e il rischio sui dati personali è Alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,0	4,2	4,6	2,2	2,9	4,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,7	4,2	4,0	2,8	2,5	3,6

Il GCRI di San Marino è 4,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 3,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (4,7/10), mentre il più basso è Supply chain (2,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Alto	Alto	Alto	Alto	Alto	Alto

La matrice applica il FOTR di 3,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per San Marino, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con San Marino, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e San Marino, La dimensione territoriale ridotta, la capacità regolatoria limitata rispetto alla portata dei progetti e la scelta di utilizzare l'intero Paese come ambiente di sperimentazione integrata producono un rischio di concentrazione non compensato dalla sola vicinanza geografica all'Italia. L'indice FOTR viene pertanto

ricalibrato a 3,8/10, imponendo una postura italiana prudenziale per dati sensibili, infrastrutture critiche e cooperazioni con accesso remoto.

Decisione operativa indicativa. Il rapporto con San Marino ricade nella fascia di alto rischio (3,8/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

separare rigorosamente reti energetiche, mobilità, servizi pubblici e dati personali;
mantenere in Italia o nel SEE chiavi, backup, amministrazione privilegiata e registri di audit;
vietare trasferimenti ulteriori e telemetria non documentata verso la Cina o altri Paesi terzi;
sottoporre firmware, aggiornamenti, centri di assistenza e componenti cloud a verifica indipendente;
prevedere portabilità, sostituzione del fornitore e disattivazione sicura testate prima dell'avvio.

Ricalibrazione 2026 di San Marino

Il punteggio 3,8/10 è motivato dalla combinazione tra: assenza di adeguatezza UE; ITU GCI Tier 4 con valori tecnici e di capacity development molto bassi; GTMI 2025 in gruppo D; limitata scala amministrativa; accordo quadro triennale con BYD per una piattaforma territoriale integrata di mobilità, energia, ricarica, omologazione e proprietà intellettuale; missione istituzionale a Shenzhen con focus su IA, robotica, batterie e infrastrutture. La riduzione non formula un giudizio sull'azienda o sulla Cina in astratto: misura il rischio di concentrazione, telemetria, firmware, manutenzione remota e trasferimenti ulteriori in un ecosistema nazionale di piccole dimensioni.

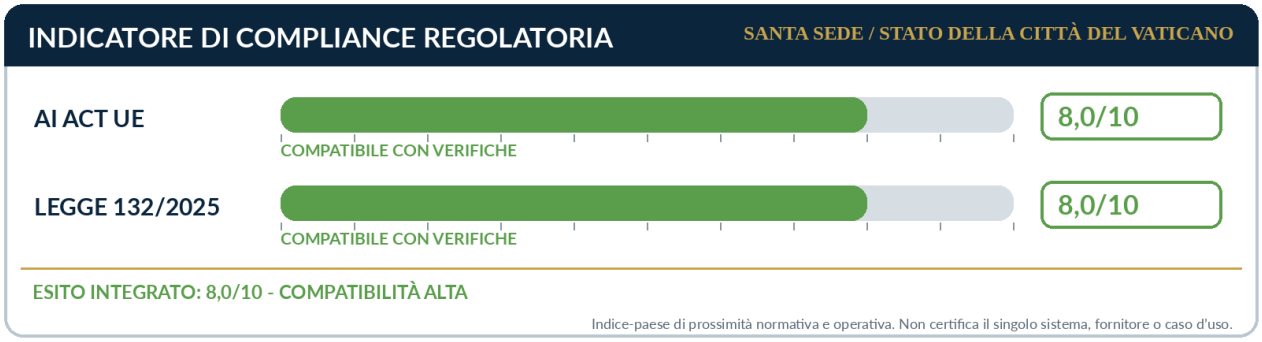
Fonti specifiche San Marino: BYD, "Accordo tra BYD e la Repubblica di San Marino", 24 marzo 2026; Segreterie di Stato / San Marino RTV, missione strategica a Shenzhen, 15 maggio 2026.

Profilo Celeborn Intelligence di San Marino: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Santa Sede / Stato della Città del Vaticano

Posizione FOTR	39	Area	Europa	Subregione	Europa meridionale
Status	Santa Sede, Stato osservatore permanente presso le Nazioni Unite	Confidenza Celeborn Intelligence	Bassa	Copertura dati	1/7 famiglie
FOTR / 10	8,0	GCRI / 10	6,8	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Santa Sede / Stato della Città del Vaticano, AI Act UE 8,0/10; legge 132/2025 8,0/10; esito integrato 8,0/10, classe «Compatibile con verifiche». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Prima dell'ingaggio occorre una analisi degli scostamenti mirata su trasparenza, governance dei dati, rappresentanza nell'UE, audit e rimedi contrattuali.

Premessa geopolitica e tecnologica

Per un operatore italiano, Santa Sede / Stato della Città del Vaticano non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La prossimità europea può ridurre i costi operativi, ma non sostituisce la verifica dell'allineamento al GDPR, delle autorità indipendenti e della reale origine dei servizi cloud. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, Russia. Per questa entità non è disponibile un indicatore Freedom in the World direttamente comparabile; l'assenza di copertura viene trattata come limite informativo e non come prova automatica di rischio. Il punteggio FOTR (8,0/10) supera il GCRI tecnico (6,8/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Santa Sede / Stato della Città del Vaticano combina buona maturità tecnologica e relativa prevedibilità normativa. Il livello di rischio aumenta nei progetti che coinvolgono dati sanitari, identità, infrastrutture critiche o ricerca strategica.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	n.d. / n.d. per 100	n.d./n.d.	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	n.d. / n.d. per milione	n.d./n.d.	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	n.d. / n.d.	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Cybersecurity	ITU GCI e tier	9,1/100 - Tier 5 - capacità iniziali	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	n.d./100 - rank n.d.	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / n.d.	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,0 / 6,4 / 5,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Santa Sede / Stato della Città del Vaticano, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 1/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Santa Sede / Stato della Città del Vaticano le evidenze principali sono GCI 9,1/100. La dimensione più robusta è capitale umano e competenze digitali (8,1/10), mentre la criticità relativa riguarda postura di sicurezza cyber (3,4/10). Sono disponibili 1 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata bassa. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Santa Sede / Stato della Città del Vaticano è 7,9/10. La base statistica rileva i principali dati WDI non sono disponibili in forma omogenea. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Per Santa Sede / Stato della Città del Vaticano non è disponibile un profilo Oxford Insights direttamente attribuibile; l'adozione di IA è quindi valutata attraverso GovTech, servizi online, infrastrutture e fonti qualitative. Il punteggio S2 è 7,9/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Santa Sede / Stato della Città del Vaticano è valutata solida, con S3 pari a 8,1/10. Le evidenze disponibili comprendono evidenza quantitativa incompleta. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Santa Sede / Stato della Città del Vaticano ottiene S4 6,8/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, Russia; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria,

repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Santa Sede / Stato della Città del Vaticano, Ecosistema multi-fornitore con dipendenze europee, statunitensi, russe o cinesi da verificare per singolo settore e livello di governo. L'impatto sulla valutazione è misurato da S4=6,8/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Santa Sede / Stato della Città del Vaticano è S5 3,4/10. La base ITU registra ITU GCI 9,1/100, Tier 5 - capacità iniziali; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è n.d.. Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Disciplina nazionale della protezione dei dati, delle comunicazioni elettroniche e dei reati informatici, con differenze rispetto al GDPR; trasferimenti e accessi pubblici richiedono una verifica locale aggiornata.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,0	Crimini finanziari	7,0
Reti criminali	4,0	Attori incorporati nello Stato	7,0
Attori stranieri	7,5	Attori del settore privato	7,0
Resilienza complessiva	6,4	Cooperazione internazionale	9,0
Politiche e norme nazionali	7,5	Forze dell'ordine	8,0
Antiriciclaggio	5,5	Prevenzione	6,0
Supporto vittime e testimoni	5,5	Rischio operativo FOTR-CY	5,8 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Santa Sede / Stato della Città del Vaticano il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,8/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 6,0/10; le frodi e i reati finanziari 7,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (7,5/10) e attori incorporati nello Stato (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Santa Sede / Stato della Città del Vaticano assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Santa Sede / Stato della Città del Vaticano, la resilienza complessiva è intermedia (6,4/10); la cooperazione internazionale è robusta (9,0/10), le politiche e norme nazionali sono robuste (7,5/10) e la capacità delle forze dell'ordine è robusta (8,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 5,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Santa Sede / Stato della Città del Vaticano, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova. Poiché l'entità non dispone di una serie nazionale GI-TOC

autonoma, i valori derivano da un proxy Celeborn Intelligence ponderato su Italia 100%; la confidenza deve pertanto essere considerata inferiore e la decisione resa più prudente.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; proxy Celeborn Intelligence ponderato su Italia 100%. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Santa Sede / Stato della Città del Vaticano, In Santa Sede / Stato della Città del Vaticano le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Santa Sede / Stato della Città del Vaticano, Il livello governativo di Santa Sede / Stato della Città del Vaticano presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Santa Sede / Stato della Città del Vaticano, Sul piano militare e dual-use, Santa Sede / Stato della Città del Vaticano mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Santa Sede / Stato della Città del Vaticano, Disciplina nazionale della protezione dei dati, delle comunicazioni elettroniche e dei reati informatici, con differenze rispetto al GDPR; trasferimenti e accessi pubblici richiedono una verifica locale aggiornata. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Santa Sede / Stato della Città del Vaticano, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 8,0/10 e il rischio sui dati personali è Medio-basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,9	7,9	8,1	6,8	3,4	6,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
7,9	7,8	8,1	8,5	7,9	8,0

Il GCRI di Santa Sede / Stato della Città del Vaticano è 6,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (8,5/10), mentre il più basso è Maturità cyber (7,8/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Santa Sede / Stato della Città del Vaticano, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Santa Sede / Stato della Città del Vaticano, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Santa Sede / Stato della Città del Vaticano, Dal punto di vista italiano, Santa Sede / Stato della Città del Vaticano rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Santa Sede / Stato della Città del Vaticano, il FOTR di 8,0/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Maturità cyber (7,8/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

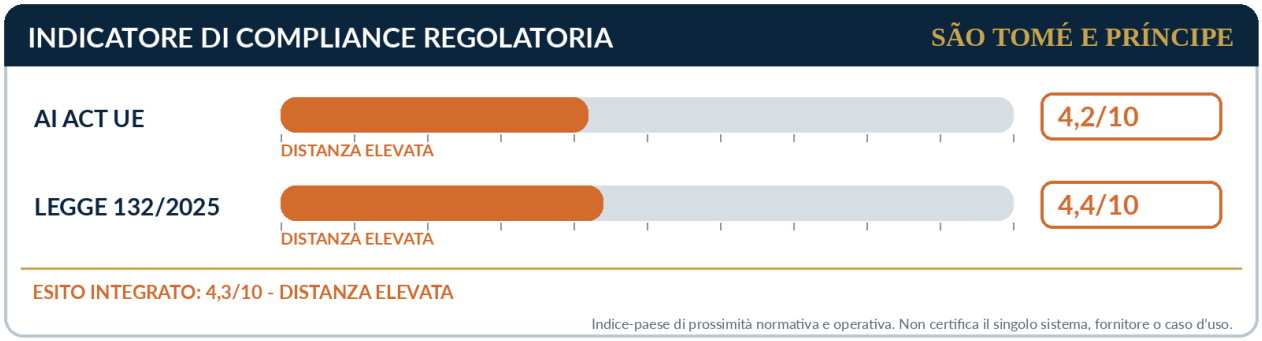
Profilo Celeborn Intelligence di Santa Sede / Stato della Città del Vaticano: World Development Indicators, valori più recenti disponibili 2022-2024; ITU Global Cybersecurity Index 2024; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Bassa con copertura 1/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.



São Tomé e Príncipe

Posizione FOTR	153	Area	Africa	Subregione	Africa centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,5	GCRI / 10	3,4	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di São Tomé e Príncipe, AI Act UE 4,2/10; legge 132/2025 4,4/10; esito integrato 4,3/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

São Tomé e Príncipe è stato membro delle nazioni unite collocato in Africa centrale. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 84/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (4,5/10) supera il GCRI tecnico (3,4/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. São Tomé e Príncipe presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	59,1% / 3,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	77,7% / 42 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	43,1 / 18,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	20,4/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	17,1/100 - rank 180	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (84/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	1,0 / 4,8 / 2,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di São Tomé e Príncipe, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per São Tomé e Príncipe le evidenze principali sono GTMI 18,7/100, EGDI 43,1/100, GCI 20,4/100, AI readiness 17,1/100. La dimensione più robusta è maturità infrastrutturale (4,5/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (1,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di São Tomé e Príncipe è 4,5/10. La base statistica rileva utenti Internet pari al 59,1% nel 2024; 3,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 77,7% nel 2024; 42 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca São Tomé e Príncipe al posto 180 con un valore medio di 17,1/100; il pilastro migliore è infrastrutture IA (29,5/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 18,7/100. Il punteggio S2 è 1,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di São Tomé e Príncipe è valutata fragile, con S3 pari a 4,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 59,3/100, sviluppo e diffusione dell'IA 10,0/100, penetrazione Internet 59,1%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di São Tomé e Príncipe ottiene S4 3,7/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di São Tomé e Príncipe, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre

ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=3,7/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di São Tomé e Príncipe è S5 2,9/10. La base ITU registra ITU GCI 20,4/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è sviluppo delle capacità (1,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (84/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	1,0	Crimini finanziari	2,5
Reti criminali	1,5	Attori incorporati nello Stato	3,0
Attori stranieri	2,0	Attori del settore privato	1,0
Resilienza complessiva	4,8	Cooperazione internazionale	7,0
Politiche e norme nazionali	7,0	Forze dell'ordine	4,5
Antiriciclaggio	3,5	Prevenzione	3,0
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	2,6 - CONTENUTO

Quadro criminale digitale. Per São Tomé e Príncipe, l'indice operativo FOTR-CY è 2,6/10, classe contenuta. Il mercato dei reati cyber-dipendenti è limitato o poco osservabile (1,0/10), mentre i crimini finanziari sono limitati o poco osservabili (2,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (3,0/10) e attori stranieri (2,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di São Tomé e Príncipe assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di São Tomé e Príncipe, la resilienza complessiva è debole (4,8/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 3,0/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in São Tomé e Príncipe, il livello contenuto non determina da solo un divieto, ma modifica il perimetro accettabile: procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di São Tomé e Príncipe. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per São Tomé e Príncipe, In São Tomé e Príncipe le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per São Tomé e Príncipe, Il livello governativo di São Tomé e Príncipe presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per São Tomé e Príncipe, Sul piano militare e dual-use, São Tomé e Príncipe mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per São Tomé e Príncipe, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso São Tomé e Príncipe, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,1/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
4,5	1,9	4,1	3,7	2,9	3,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,7	4,3	4,5	5,2	3,7	4,1

Il GCRI di São Tomé e Príncipe è 3,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,2/10), mentre il più basso è Supply chain (3,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per São Tomé e Príncipe, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con São Tomé e Príncipe, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e São Tomé e Príncipe, Dal punto di vista italiano, São Tomé e Príncipe rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con São Tomé e Príncipe ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

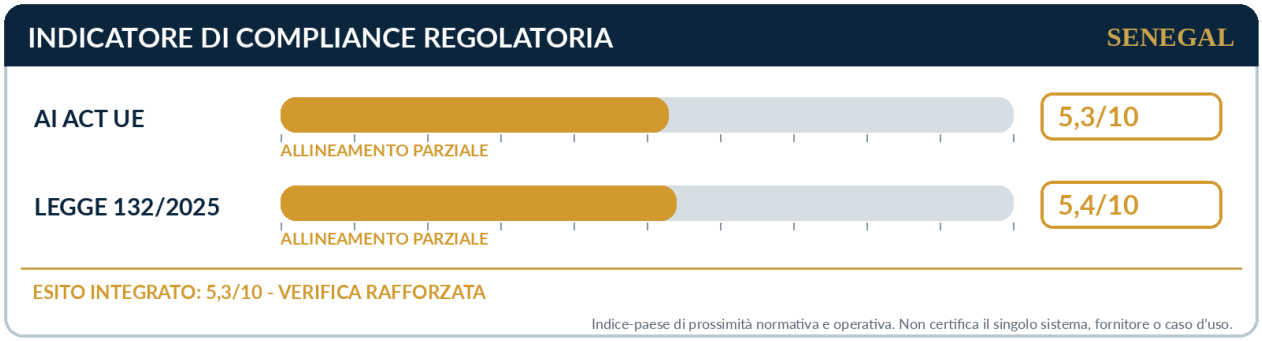
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di São Tomé e Príncipe: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Senegal

Posizione FOTR	123	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,4	GCRI / 10	5,0	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Senegal, AI Act UE 5,3/10; legge 132/2025 5,4/10; esito integrato 5,3/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Senegal presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 70/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,0/10) e indice FOTR (5,4/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Senegal presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	60,1% / 4,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	82,9% / 60 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	51,6 / 43,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	67,2/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	43,0/100 - rank 96	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (70/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 5,9 / 5,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Senegal, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Senegal le evidenze principali sono GTMI 43,4/100, EGDI 51,6/100, GCI 67,2/100, AI readiness 43,0/100. La dimensione più robusta è postura di sicurezza cyber (6,2/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (4,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Senegal è 5,5/10. La base statistica rileva utenti Internet pari al 60,1% nel 2024; 4,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 82,9% nel 2024; 60 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Senegal al posto 96 con un valore medio di 43,0/100; il pilastro migliore è governance (63,4/100), quello più debole è adozione pubblica (28,5/100). Il GTMI 2025 è 43,4/100. Il punteggio S2 è 4,3/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Senegal è valutata fragile, con S3 pari a 4,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 33,8/100, sviluppo e diffusione dell'IA 31,4/100, penetrazione Internet 60,1%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Senegal ottiene S4 4,9/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Senegal, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,9/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Senegal è S5 6,2/10. La base ITU registra ITU GCI 67,2/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è organizzazione (9,1/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (70/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge 2008-12 sulla protezione dei dati e strategia cyber; capacità in crescita, ma infrastrutture e vigilanza restano variabili.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	6,0
Reti criminali	6,0	Attori incorporati nello Stato	5,5
Attori stranieri	6,5	Attori del settore privato	6,5
Resilienza complessiva	5,9	Cooperazione internazionale	7,0
Politiche e norme nazionali	6,5	Forze dell'ordine	6,0
Antiriciclaggio	5,5	Prevenzione	5,0
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	5,2 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Senegal restituisce un rischio FOTR-CY di 5,2/10 (significativo). La componente cyber-dipendente vale 5,0/10 e quella finanziaria 6,0/10; la risposta sistemica è valutata intermedia, con resilienza media di 5,9/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (6,5/10) e attori del settore privato (6,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Senegal assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Senegal, la resilienza complessiva è intermedia (5,9/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è intermedia (6,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 5,0/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Senegal, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Senegal. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Senegal, In Senegal le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La superficie di

rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Senegal, Il livello governativo di Senegal presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Senegal, Sul piano militare e dual-use, Senegal mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Senegal, Legge 2008-12 sulla protezione dei dati e strategia cyber; capacità in crescita, ma infrastrutture e vigilanza restano variabili. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Senegal, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,0/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
5,5	4,3	4,1	4,9	6,2	5,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,6	5,1	5,5	5,9	5,2	5,0

Il GCRI di Senegal è 5,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,9/10), mentre il più basso è Trasferibilità dati (5,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio

La matrice applica il FOTR di 5,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Senegal, 5 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Senegal, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Senegal, Dal punto di vista italiano, Senegal rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Senegal è indicata una cooperazione selettiva, coerente con il FOTR di 5,4/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

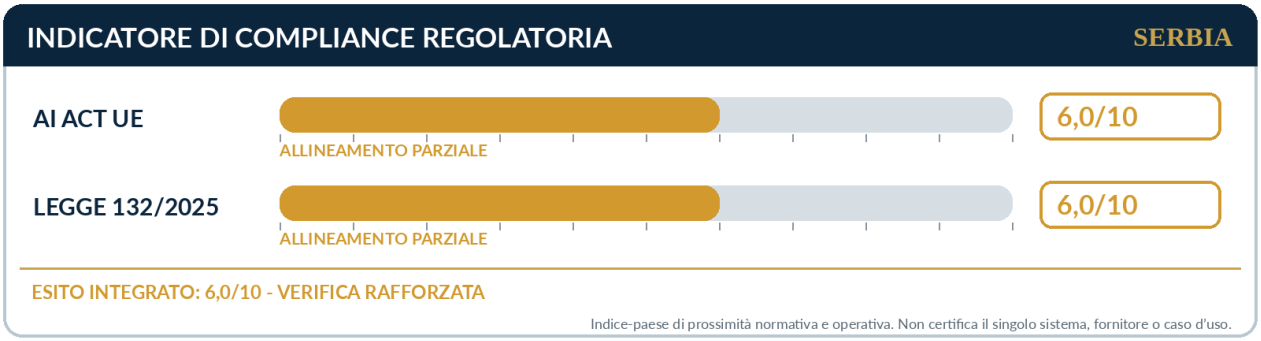
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Senegal: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Serbia

Posizione FOTR	79	Area	Europa	Subregione	Europa sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,9	GCRI / 10	7,4	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Serbia, AI Act UE 6,0/10; legge 132/2025 6,0/10; esito integrato 6,0/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Serbia, situato in Europa sud-orientale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La prossimità europea può ridurre i costi operativi, ma non sostituisce la verifica dell'allineamento al GDPR, delle autorità indipendenti e della reale origine dei servizi cloud. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Cina, Russia, Turchia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 53/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (7,4/10) è superiore al punteggio FOTR (5,9/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Il quadro di Serbia è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	87,7% / 33,4 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 12.942 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	86,2 / 97,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	96,8/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	65,9/100 - rank 40	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	67/100 - Parzialmente libero / Parzialmente libero (53/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 4,9 / 6,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Serbia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Serbia le evidenze principali sono GTMI 97,7/100, EGDI 86,2/100, GCI 96,8/100, AI readiness 65,9/100. La dimensione più robusta è maturità infrastrutturale (8,9/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,3/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Serbia è 8,9/10. La base statistica rileva utenti Internet pari al 87,7% nel 2024; 33,4 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 12.942 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Serbia al posto 40 con un valore medio di 65,9/100; il pilastro migliore è politiche pubbliche (100,0/100), quello più debole è sviluppo e diffusione (35,8/100). Il GTMI 2025 è 97,7/100. Il punteggio S2 è 7,3/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Serbia è valutata sufficiente ma disomogenea, con S3 pari a 6,6/10. Le evidenze disponibili comprendono indice UN di capitale umano 80,9/100, sviluppo e diffusione dell'IA 35,8/100, penetrazione Internet 87,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Serbia ottiene S4 6,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Cina, Russia, Turchia; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Serbia, Mercato multi-fornitore tra Unione europea, Stati Uniti, Turchia, Cina e, in alcuni segmenti, Russia; il peso relativo varia tra pubblico, telecomunicazioni e difesa. L'impatto sulla valutazione è misurato

da S4=6,3/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Serbia è S5 7,8/10. La base ITU registra ITU GCI 96,8/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure tecniche (18,4/20). Freedom on the Net è 67/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (53/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Quadro nazionale di protezione dati e cybersicurezza in progressivo allineamento all'acquis dell'Unione europea; la distanza tra legge formale, vigilanza e prassi deve essere verificata nel settore interessato.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	7,0
Reti criminali	7,0	Attori incorporati nello Stato	8,0
Attori stranieri	6,5	Attori del settore privato	6,0
Resilienza complessiva	4,9	Cooperazione internazionale	6,5
Politiche e norme nazionali	4,5	Forze dell'ordine	5,0
Antiriciclaggio	5,5	Prevenzione	5,5
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	6,0 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Serbia il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 6,0/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 5,0/10; le frodi e i reati finanziari 7,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e reti criminali (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Serbia assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Serbia, la resilienza complessiva è debole (4,9/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono deboli (4,5/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 5,5/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Serbia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Serbia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Serbia, In Serbia le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Serbia, Il livello governativo di Serbia presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Serbia, Sul piano militare e dual-use, Serbia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Serbia, Quadro nazionale di protezione dati e cybersicurezza in progressivo allineamento all'acquis dell'Unione europea; la distanza tra legge formale, vigilanza e prassi deve essere verificata nel settore interessato. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Serbia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,5/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,9	7,3	6,6	6,3	7,8	7,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,3	5,5	5,4	6,8	5,7	5,5

Il GCRI di Serbia è 7,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,9/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,8/10), mentre il più basso è Trasparenza istituzionale (5,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,9/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Serbia, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Serbia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Serbia, Dal punto di vista italiano, Serbia rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Serbia è indicata una cooperazione selettiva, coerente con il FOTR di 5,9/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasparenza istituzionale a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

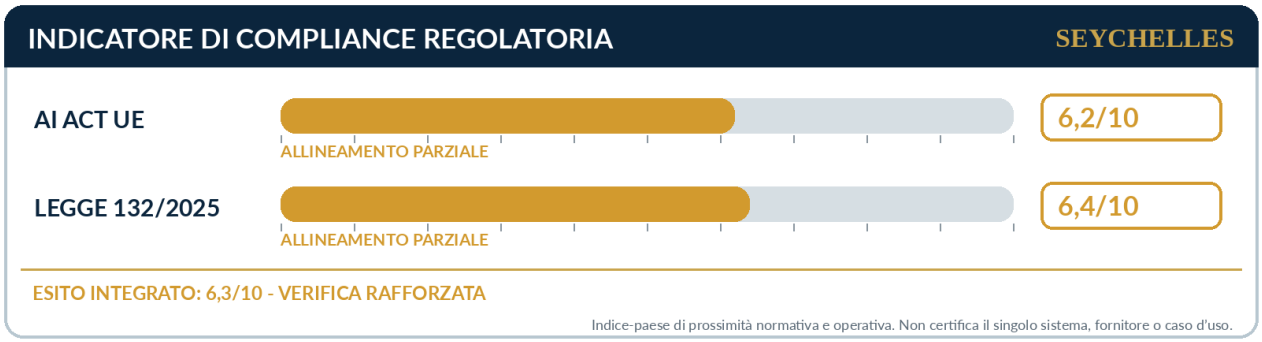
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Serbia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Seychelles

Posizione FOTR	59	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	6,5	GCRI / 10	5,5	Classe operativa	Affidabilità favorevole ma condizionata

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Seychelles, AI Act UE 6,2/10; legge 132/2025 6,4/10; esito integrato 6,3/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Seychelles non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 81/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (6,5/10) supera il GCRI tecnico (5,5/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il quadro di Seychelles è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	87,8% / 31,6 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 139.583 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	67,7 / 35,1	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	50,3/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	26,0/100 - rank 140	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (81/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Firmatario/invitato	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 5,4 / 4,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Seychelles, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Seychelles le evidenze principali sono GTMI 35,1/100, EGDI 67,7/100, GCI 50,3/100, AI readiness 26,0/100. La dimensione più robusta è maturità infrastrutturale (9,0/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,2/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Seychelles è 9,0/10. La base statistica rileva utenti Internet pari al 87,8% nel 2024; 31,6 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 139.583 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Seychelles al posto 140 con un valore medio di 26,0/100; il pilastro migliore è infrastrutture IA (43,8/100), quello più debole è politiche pubbliche (8,0/100). Il GTMI 2025 è 35,1/100. Il punteggio S2 è 3,2/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Seychelles è valutata sufficiente ma disomogenea, con S3 pari a 5,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 67,7/100, sviluppo e diffusione dell'IA 11,8/100, penetrazione Internet 87,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Seychelles ottiene S4 4,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Seychelles, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre

ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,6/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Seychelles è S5 5,5/10. La base ITU registra ITU GCI 50,3/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (3,2/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (81/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Firmatario/invitato. Quadro normativo sintetico: Data Protection Act e quadro cyber in aggiornamento; piccola scala amministrativa e dipendenza da fornitori esterni.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	5,5
Reti criminali	5,0	Attori incorporati nello Stato	4,0
Attori stranieri	5,0	Attori del settore privato	4,0
Resilienza complessiva	5,4	Cooperazione internazionale	6,5
Politiche e norme nazionali	5,5	Forze dell'ordine	5,0
Antiriciclaggio	5,0	Prevenzione	5,0
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	4,0 - MODERATO

Rischio criminale connesso alle tecnologie. In Seychelles il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 4,0/10, livello moderato. I reati che dipendono direttamente da sistemi informatici raggiungono 2,0/10; le frodi e i reati finanziari 5,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (5,0/10) e attori stranieri (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Seychelles assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Seychelles, la resilienza complessiva è debole (5,4/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 5,0/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Seychelles, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Seychelles. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Seychelles, In Seychelles le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Seychelles, Il livello governativo di Seychelles presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il

settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Seychelles, Sul piano militare e dual-use, Seychelles mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Seychelles, Data Protection Act e quadro cyber in aggiornamento; piccola scala amministrativa e dipendenza da fornitori esterni. Lo stato rispetto alla Convenzione di Budapest è: Firmatario/invitato; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Seychelles, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 6,6/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,0	3,2	5,0	4,6	5,5	5,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,6	6,0	6,6	7,4	6,0	6,6

Il GCRI di Seychelles è 5,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (7,4/10), mentre il più basso è Maturità cyber (6,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Seychelles, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Seychelles, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Seychelles, Dal punto di vista italiano, Seychelles rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Seychelles è favorevole ma condizionata: il valore FOTR di 6,5/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Maturità cyber.

Presidi minimi raccomandati

- Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
- Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
- Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
- Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

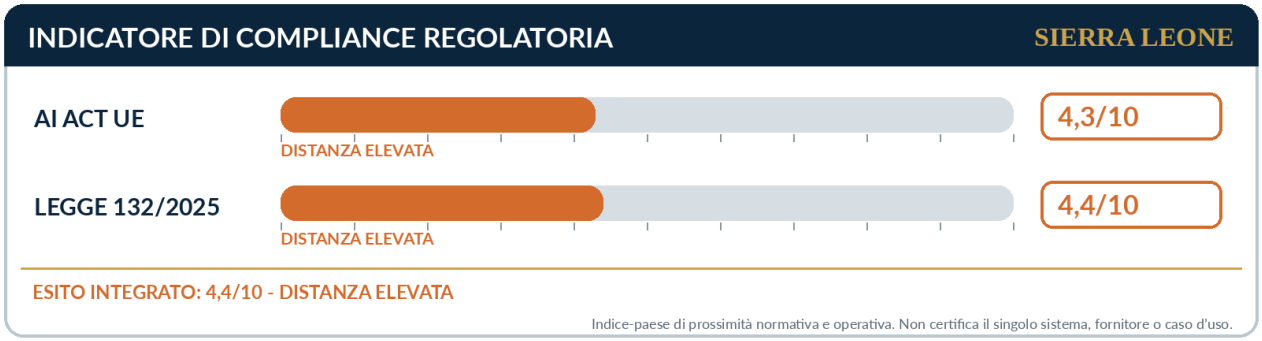
Profilo Celeborn Intelligence di Seychelles: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025;

Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Sierra Leone

Posizione FOTR	152	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,5	GCRI / 10	3,4	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Sierra Leone, AI Act UE 4,3/10; legge 132/2025 4,4/10; esito integrato 4,4/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Sierra Leone è stato membro delle nazioni unite collocato in Africa occidentale. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 61/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (4,5/10) supera il GCRI tecnico (3,4/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Per Sierra Leone non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	25,1% / 0,0 per 100	2024/2021	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	39,2% / 11 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	30,4 / 42,1	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	56,5/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	21,1/100 - rank 175	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (61/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,5 / 4,0 / 5,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Sierra Leone, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Sierra Leone le evidenze principali sono GTMI 42,1/100, EGDI 30,4/100, GCI 56,5/100, AI readiness 21,1/100. La dimensione più robusta è postura di sicurezza cyber (5,2/10), mentre la criticità relativa riguarda maturità infrastrutturale (2,2/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Sierra Leone è 2,2/10. La base statistica rileva utenti Internet pari al 25,1% nel 2024; 0,0 abbonamenti fissi ogni 100 abitanti nel 2021; accesso all'elettricità del 39,2% nel 2024; 11 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Sierra Leone al posto 175 con un valore medio di 21,1/100; il pilastro migliore è resilienza (31,2/100), quello più debole è sviluppo e diffusione (10,9/100). Il GTMI 2025 è 42,1/100. Il punteggio S2 è 2,8/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Sierra Leone è valutata fragile, con S3 pari a 2,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 27,2/100, sviluppo e diffusione dell'IA 10,9/100, penetrazione Internet 25,1%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Sierra Leone ottiene S4 4,5/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Sierra Leone, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre

ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,5/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Sierra Leone è S5 5,2/10. La base ITU registra ITU GCI 56,5/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (1,4/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (61/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,5	Crimini finanziari	5,0
Reti criminali	6,5	Attori incorporati nello Stato	8,0
Attori stranieri	7,5	Attori del settore privato	4,0
Resilienza complessiva	4,0	Cooperazione internazionale	5,0
Politiche e norme nazionali	4,0	Forze dell'ordine	4,5
Antiriciclaggio	4,5	Prevenzione	4,5
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	5,2 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Sierra Leone il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,2/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 2,5/10; le frodi e i reati finanziari 5,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e attori stranieri (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Sierra Leone assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Sierra Leone, la resilienza complessiva è debole (4,0/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono deboli (4,0/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 4,5/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Sierra Leone, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Sierra Leone. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Sierra Leone, In Sierra Leone le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La

disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Sierra Leone, Il livello governativo di Sierra Leone presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Sierra Leone, Sul piano militare e dual-use, Sierra Leone mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Sierra Leone, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Sierra Leone, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,2/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
2,2	2,8	2,4	4,5	5,2	3,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,7	4,5	4,1	5,1	4,0	4,2

Il GCRI di Sierra Leone è 3,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,1/10), mentre il più basso è Supply chain (4,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Sierra Leone, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Sierra Leone, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Sierra Leone, Dal punto di vista italiano, Sierra Leone rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Sierra Leone ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

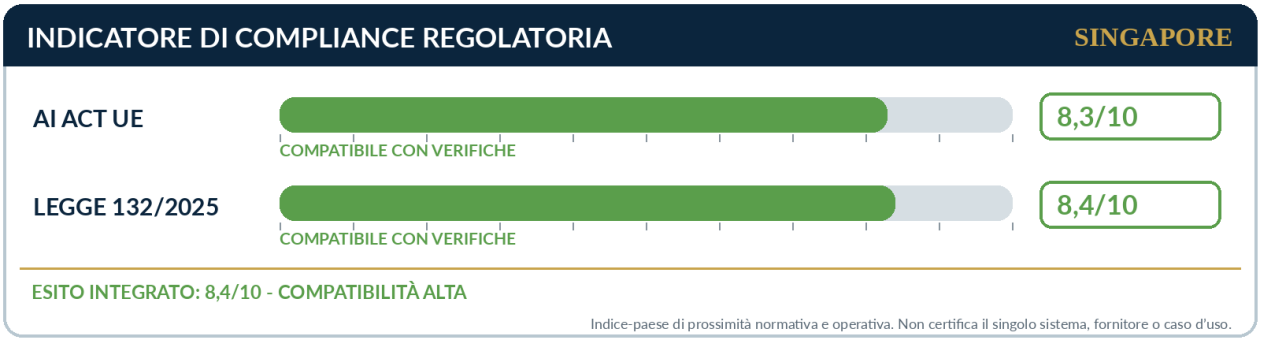
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Sierra Leone: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Singapore

Posizione FOTR	29	Area	Asia	Subregione	Asia sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	8,4	GCRI / 10	8,6	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Singapore, AI Act UE 8,3/10; legge 132/2025 8,4/10; esito integrato 8,4/10, classe «Compatibile con verifiche». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Prima dell'ingaggio occorre una analisi degli scostamenti mirata su trasparenza, governance dei dati, rappresentanza nell'UE, audit e rimedi contrattuali.

Premessa geopolitica e tecnologica

Singapore svolge il ruolo di hub digitale, finanziario, logistico e cloud dell'Asia sud-orientale. La qualità delle infrastrutture e della regolazione è elevata, ma la sua funzione di nodo regionale implica flussi transfrontalieri complessi, dipendenze dagli hyperscaler e una fitta rete di subfornitori. Per l'Italia è un ambiente favorevole, purché siano mappati Paesi di transito, accessi remoti e regole applicabili ai dati trasferiti verso altri mercati asiatici. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 48/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,6/10) e indice FOTR (8,4/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Hub cloud, finanziario e logistico di primo livello; l'eccellenza operativa va accompagnata da analisi degli accessi pubblici e dei trasferimenti successivi verso altre giurisdizioni asiatiche.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	94,4% / 27,8 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 209.665 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	96,9 / 92,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	99,9/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	78,5/100 - rank 7	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	53/100 - Parzialmente libero / Parzialmente libero (48/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,0 / 7,8 / 4,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Singapore, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Singapore le evidenze principali sono GTMI 92,7/100, EGDI 96,9/100, GCI 99,9/100, AI readiness 78,5/100. La dimensione più robusta è maturità infrastrutturale (9,3/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (8,1/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Singapore è 9,3/10. La base statistica rileva utenti Internet pari al 94,4% nel 2024; 27,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 209.665 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Singapore al posto 7 con un valore medio di 78,5/100; il pilastro migliore è adozione pubblica (92,5/100), quello più debole è sviluppo e diffusione (64,2/100). Il GTMI 2025 è 92,7/100. Il punteggio S2 è 8,3/10 e indica una capacità elevata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Singapore è valutata solida, con S3 pari a 8,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 93,6/100, sviluppo e diffusione dell'IA 64,2/100, penetrazione Internet 94,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Singapore ottiene S4 8,5/10 e presenta buona capacità di diversificazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, Giappone/Corea; l'indicatore di indipendenza disponibile è 8,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Singapore, Hub multi-fornitore con prevalenza di gruppi statunitensi, europei, giapponesi, coreani e cinesi, sottoposti a governance locale sofisticata. L'impatto sulla valutazione è misurato da S4=8,5/10 e dal proxy di indipendenza 8,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Singapore è S5 8,6/10. La base ITU registra ITU GCI 99,9/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è sviluppo delle capacità (19,9/20). Freedom on the Net è 53/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (48/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Personal Data Protection Act, Cybersecurity Act e regole per infrastrutture critiche; trasferimenti UE con SCC/TIA e controllo degli accessi pubblici.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,0	Crimini finanziari	6,0
Reti criminali	5,0	Attori incorporati nello Stato	1,5
Attori stranieri	4,5	Attori del settore privato	3,5
Resilienza complessiva	7,8	Cooperazione internazionale	9,0
Politiche e norme nazionali	8,5	Forze dell'ordine	9,0
Antiriciclaggio	7,5	Prevenzione	9,0
Supporto vittime e testimoni	7,0	Rischio operativo FOTR-CY	4,7 - MODERATO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (7,0/10), criminalità finanziaria (6,0/10) e resilienza (7,8/10) colloca Singapore in una fascia di rischio moderato, pari a 4,7/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (5,0/10) e attori stranieri (4,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Singapore assumono particolare rilevanza centri organizzati di truffa, frodi d'investimento e sentimentali, phishing multicanale, batterie di schede SIM, conti prestanome, riciclaggio in cripto-attività e compromissione di servizi esternalizzati. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Singapore, la resilienza complessiva è robusta (7,8/10); la cooperazione internazionale è robusta (9,0/10), le politiche e norme nazionali sono robuste (8,5/10) e la capacità delle forze dell'ordine è robusta (9,0/10). Completano il quadro antiriciclaggio 7,5/10, prevenzione 9,0/10 e supporto a vittime e testimoni 7,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Singapore, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; controllo della filiera contro esposizione a complessi organizzati per truffe telematiche, call center coercitivi e conti prestanome.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Singapore. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Singapore, In Singapore le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Singapore, Il livello governativo di Singapore presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Singapore, Sul piano militare e dual-use, Singapore mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano

controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Singapore, Personal Data Protection Act, Cybersecurity Act e regole per infrastrutture critiche; trasferimenti UE con SCC/TIA e controllo degli accessi pubblici. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Singapore, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 7,4/10 e il rischio sui dati personali è Medio-basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,3	8,3	8,1	8,5	8,6	8,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,7	9,6	7,4	8,1	9,1	7,4

Il GCRI di Singapore è 8,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Maturità cyber (9,6/10), mentre il più basso è Trasparenza istituzionale (7,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-basso	Medio-basso	Basso	Medio-basso	Basso	Medio-basso

La matrice applica il FOTR di 8,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Singapore, la cautela si concentra su 4 ambiti a rischio intermedio: Dati personali, Sanità e biometria, IP e R&S, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Singapore, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Singapore, Dal punto di vista italiano, Singapore rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Singapore, il FOTR di 8,4/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (7,4/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

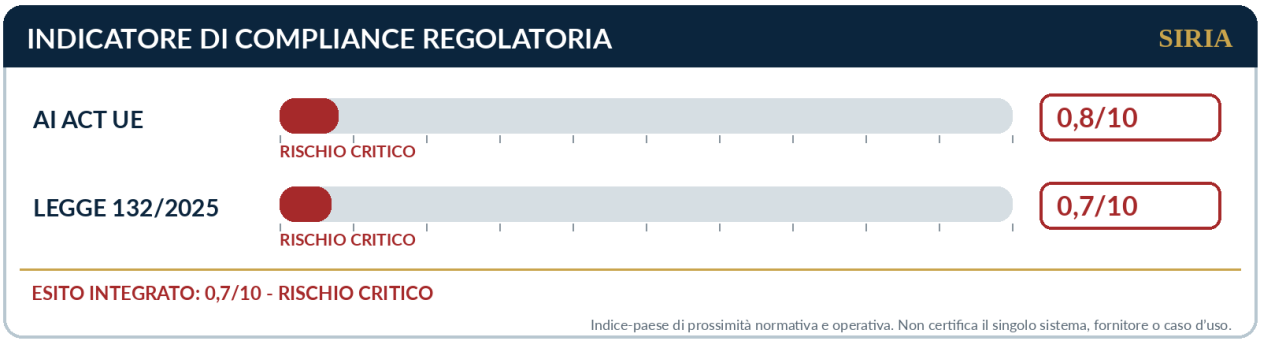
- Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
- Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
- Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
- Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Singapore: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Siria

Posizione FOTR	207	Area	Asia	Subregione	Medio Oriente e Asia occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	0,6	GCRI / 10	2,8	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Siria, AI Act UE 0,8/10; legge 132/2025 0,7/10; esito integrato 0,7/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Siria, situato in Medio Oriente e Asia occidentale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 10/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (2,8/10) è superiore al punteggio FOTR (0,6/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Per Siria la regola operativa è evitare trasferimenti e dipendenze tecnologiche, salvo finalità umanitarie o istituzionali autorizzate e protette da architetture isolate. Il contratto, da solo, non rende il rischio accettabile.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	33,8% / 6,9 per 100	2018/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	89,3% / 114 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	38,9 / 5,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	51,4/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	20,6/100 - rank 165	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (10/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,0 / 2,0 / 7,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Siria, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Siria le evidenze principali sono GTMI 5,3/100, EGDI 38,9/100, GCI 51,4/100, AI readiness 20,6/100. La dimensione più robusta è maturità infrastrutturale (3,7/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,0/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Siria è 3,7/10. La base statistica rileva utenti Internet pari al 33,8% nel 2018; 6,9 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 89,3% nel 2024; 114 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Siria al posto 165 con un valore medio di 20,6/100; il pilastro migliore è infrastrutture IA (33,2/100), quello più debole è politiche pubbliche (4,0/100). Il GTMI 2025 è 5,3/100. Il punteggio S2 è 2,0/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Siria è valutata fragile, con S3 pari a 2,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 41,7/100, sviluppo e diffusione dell'IA 16,8/100, penetrazione Internet 33,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Siria ottiene S4 2,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Siria, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo societario e

subfornitura. L'impatto sulla valutazione è misurato da S4=2,6/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Siria è S5 2,8/10. La base ITU registra ITU GCI 51,4/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è cooperazione (5,5/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (10/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa e infrastrutture in contesto di conflitto, controllo statale e sanzioni; criticità estreme per ogni flusso di dati e tecnologia.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,0	Crimini finanziari	8,0
Reti criminali	8,5	Attori incorporati nello Stato	10,0
Attori stranieri	8,0	Attori del settore privato	7,0
Resilienza complessiva	2,0	Cooperazione internazionale	4,0
Politiche e norme nazionali	2,0	Forze dell'ordine	2,0
Antiriciclaggio	2,0	Prevenzione	2,0
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	7,2 - ALTO

Quadro criminale digitale. Per Siria, l'indice operativo FOTR-CY è 7,2/10, classe alta. Il mercato dei reati cyber-dipendenti è intermedio (4,0/10), mentre i crimini finanziari sono molto elevati (8,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (10,0/10) e reti criminali (8,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Siria assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Siria, la resilienza complessiva è molto debole (2,0/10); la cooperazione internazionale è debole (4,0/10), le politiche e norme nazionali sono molto deboli (2,0/10) e la capacità delle forze dell'ordine è molto debole (2,0/10). Completano il quadro antiriciclaggio 2,0/10, prevenzione 2,0/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Siria, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Siria. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Siria, In Siria le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. La

disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Siria, Il livello governativo di Siria presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Siria, Sul piano militare e dual-use, Siria mostra capacità domestiche e cooperazione con partner soggetti a sanzioni o restrizioni. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Siria, Normativa e infrastrutture in contesto di conflitto, controllo statale e sanzioni; criticità estreme per ogni flusso di dati e tecnologia. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Siria, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 0,0/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,7	2,0	2,8	2,6	2,8	2,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
1,2	1,5	0,0	0,0	0,5	0,0

Il GCRI di Siria è 2,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 0,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (1,5/10), mentre il più basso è Trasparenza istituzionale (0,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 0,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Siria, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Siria, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Siria, Dal punto di vista italiano, Siria rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Siria, il FOTR di 0,6/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

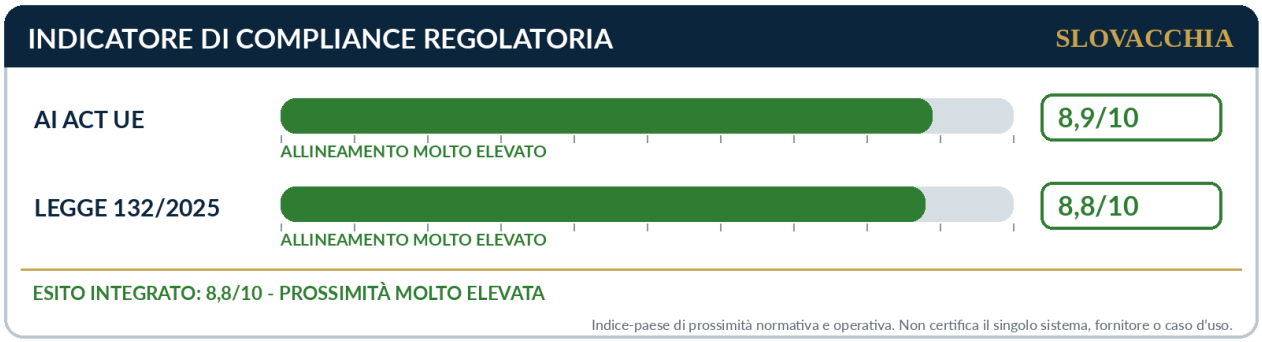
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Siria: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Slovacchia

Posizione FOTR	33	Area	Europa	Subregione	Europa occidentale e centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,2	GCRI / 10	7,2	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Slovacchia, AI Act UE 8,9/10; legge 132/2025 8,8/10; esito integrato 8,8/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Per un operatore italiano, Slovacchia non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 88/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (8,2/10) supera il GCRI tecnico (7,2/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Slovacchia combina buona maturità tecnologica e relativa prevedibilità normativa. Il livello di rischio aumenta nei progetti che coinvolgono dati sanitari, identità, infrastrutture critiche o ricerca strategica.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	89,8% / 33,8 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 43.287 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	80,2 / 66,1	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	94,4/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	47,9/100 - rank 73	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (88/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,0 / 4,9 / 5,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Slovacchia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Slovacchia le evidenze principali sono GTMI 66,1/100, EGDI 80,2/100, GCI 94,4/100, AI readiness 47,9/100. La dimensione più robusta è maturità infrastrutturale (9,0/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (5,5/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Slovacchia è 9,0/10. La base statistica rileva utenti Internet pari al 89,8% nel 2024; 33,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 43.287 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Slovacchia al posto 73 con un valore medio di 47,9/100; il pilastro migliore è governance (72,5/100), quello più debole è politiche pubbliche (19,0/100). Il GTMI 2025 è 66,1/100. Il punteggio S2 è 5,5/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Slovacchia è valutata sufficiente ma disomogenea, con S3 pari a 6,7/10. Le evidenze disponibili comprendono indice UN di capitale umano 79,8/100, sviluppo e diffusione dell'IA 31,4/100, penetrazione Internet 89,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Slovacchia ottiene S4 6,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Slovacchia, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo

societario, luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Slovacchia è S5 8,7/10. La base ITU registra ITU GCI 94,4/100, Tier 2 - avanzato; il pilastro relativamente più debole è cooperazione (16,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (88/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, legge 18/2018 e Cybersecurity Act; adeguamento a NIS2 e CER.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,0	Crimini finanziari	6,5
Reti criminali	5,5	Attori incorporati nello Stato	7,0
Attori stranieri	5,5	Attori del settore privato	3,0
Resilienza complessiva	4,9	Cooperazione internazionale	6,0
Politiche e norme nazionali	6,0	Forze dell'ordine	4,5
Antiriciclaggio	5,0	Prevenzione	5,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	5,9 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Slovacchia presenta un'esposizione stimata significativa (5,9/10): reati cyber-dipendenti 6,0/10, crimini finanziari 6,5/10 e resilienza 4,9/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,0/10) e reti criminali (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Slovacchia assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Slovacchia, la resilienza complessiva è debole (4,9/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 5,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Slovacchia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Slovacchia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Slovacchia, In Slovacchia le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Slovacchia, Il livello governativo di Slovacchia presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Slovacchia, Sul piano militare e dual-use, Slovacchia mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Slovacchia, GDPR, legge 18/2018 e Cybersecurity Act; adeguamento a NIS2 e CER. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Slovacchia, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,1/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,0	5,5	6,7	6,1	8,7	7,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,8	7,2	7,7	8,6	7,7	9,1

Il GCRI di Slovacchia è 7,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,1/10), mentre il più basso è Maturità cyber (7,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Slovacchia, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Slovacchia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Slovacchia, Dal punto di vista italiano, Slovacchia rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Slovacchia, il FOTR di 8,2/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Maturità cyber (7,2/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

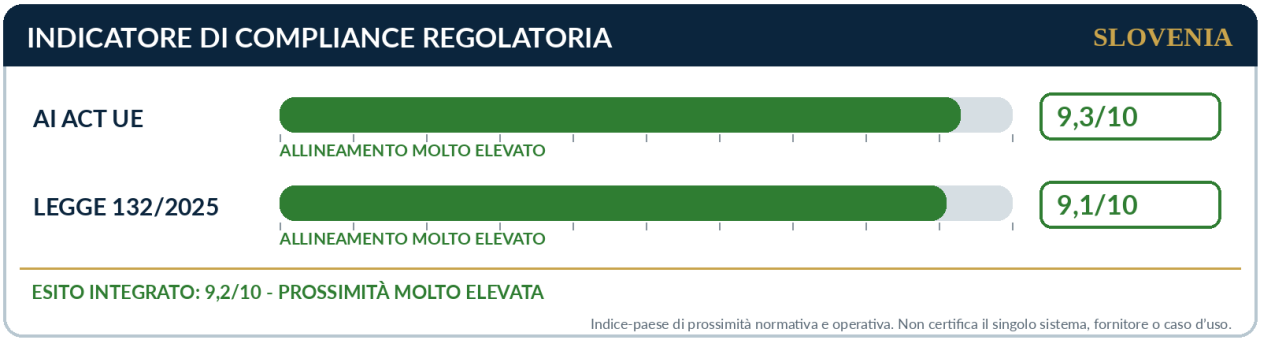
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Slovacchia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Slovenia

Posizione FOTR	27	Area	Europa	Subregione	Europa sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,5	GCRI / 10	7,8	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Slovenia, AI Act UE 9,3/10; legge 132/2025 9,1/10; esito integrato 9,2/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Slovenia è stato membro delle nazioni unite collocato in Europa sud-orientale. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 97/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,8/10) e indice FOTR (8,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il sistema digitale di Slovenia è avanzato e integrato con standard internazionali. Le principali criticità non sono di base istituzionale, ma riguardano supply chain, concentrazione dei servizi e gestione delle eccezioni di sicurezza nazionale.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	90,8% / 34,2 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 68.783 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	87,6 / 88,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	96,5/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	66,2/100 - rank 36	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (97/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 6,2 / 5,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Slovenia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Slovenia le evidenze principali sono GTMI 88,2/100, EGDI 87,6/100, GCI 96,5/100, AI readiness 66,2/100. La dimensione più robusta è maturità infrastrutturale (9,2/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,2/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Slovenia è 9,2/10. La base statistica rileva utenti Internet pari al 90,8% nel 2024; 34,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 68.783 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Slovenia al posto 36 con un valore medio di 66,2/100; il pilastro migliore è politiche pubbliche (84,0/100), quello più debole è sviluppo e diffusione (45,5/100). Il GTMI 2025 è 88,2/100. Il punteggio S2 è 7,2/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Slovenia è valutata sufficiente ma disomogenea, con S3 pari a 7,3/10. Le evidenze disponibili comprendono indice UN di capitale umano 85,3/100, sviluppo e diffusione dell'IA 45,5/100, penetrazione Internet 90,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Slovenia ottiene S4 6,2/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Slovenia, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,2/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Slovenia è S5 9,0/10. La base ITU registra ITU GCI 96,5/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è organizzazione (18,2/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (97/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, ZVOP-2 e disciplina nazionale cyber; applicazione del corpus UE.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	6,5
Reti criminali	5,0	Attori incorporati nello Stato	6,5
Attori stranieri	5,5	Attori del settore privato	4,0
Resilienza complessiva	6,2	Cooperazione internazionale	7,0
Politiche e norme nazionali	7,0	Forze dell'ordine	6,0
Antiriciclaggio	5,5	Prevenzione	6,0
Supporto vittime e testimoni	6,0	Rischio operativo FOTR-CY	5,1 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (5,0/10), criminalità finanziaria (6,5/10) e resilienza (6,2/10) colloca Slovenia in una fascia di rischio significativo, pari a 5,1/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (6,5/10) e attori stranieri (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Slovenia assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Slovenia, la resilienza complessiva è intermedia (6,2/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è intermedia (6,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 6,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Slovenia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Slovenia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Slovenia, In Slovenia le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Slovenia, Il livello governativo di Slovenia presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Slovenia, Sul piano militare e dual-use, Slovenia mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Slovenia, GDPR, ZVOP-2 e disciplina nazionale cyber; applicazione del corpus UE. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Slovenia, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,6/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,2	7,2	7,3	6,2	9,0	7,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,0	7,7	7,9	9,0	7,8	9,6

Il GCRI di Slovenia è 7,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,6/10), mentre il più basso è Maturità cyber (7,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Slovenia, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Slovenia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Slovenia, Dal punto di vista italiano, Slovenia rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Slovenia, il FOTR di 8,5/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Maturità cyber (7,7/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

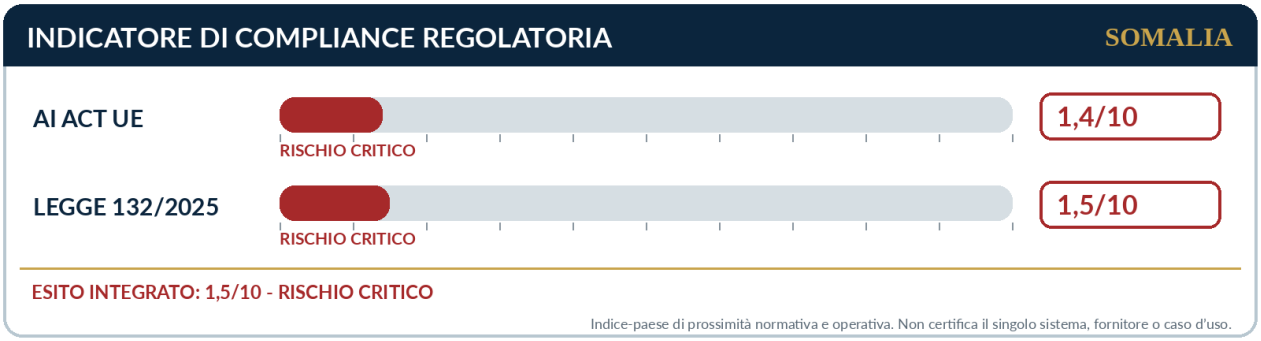
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Slovenia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Somalia

Posizione FOTR	199	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	1,3	GCRI / 10	1,8	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Somalia, AI Act UE 1,4/10; legge 132/2025 1,5/10; esito integrato 1,5/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Somalia presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 8/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (1,8/10) e indice FOTR (1,3/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per Somalia la regola operativa è evitare trasferimenti e dipendenze tecnologiche, salvo finalità umanitarie o istituzionali autorizzate e protette da architetture isolate. Il contratto, da solo, non rende il rischio accettabile.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	27,9% / 0,7 per 100	2024/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	54,4% / 14 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	14,7 / 10,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	37,4/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	21,5/100 - rank 164	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (8/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,5 / 1,9 / 6,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Somalia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Somalia le evidenze principali sono GTMI 10,2/100, EGDI 14,7/100, GCI 37,4/100, AI readiness 21,5/100. La dimensione più robusta è indipendenza della supply chain (2,6/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (1,0/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Somalia è 1,6/10. La base statistica rileva utenti Internet pari al 27,9% nel 2024; 0,7 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 54,4% nel 2024; 14 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Somalia al posto 164 con un valore medio di 21,5/100; il pilastro migliore è resilienza (29,9/100), quello più debole è adozione pubblica (11,2/100). Il GTMI 2025 è 10,2/100. Il punteggio S2 è 2,1/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Somalia è valutata fragile, con S3 pari a 1,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 0,0/100, sviluppo e diffusione dell'IA 22,3/100, penetrazione Internet 27,9%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Somalia ottiene S4 2,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Somalia, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=2,6/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Somalia è S5 1,8/10. La base ITU registra ITU GCI 37,4/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è sviluppo delle capacità (4,3/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (8/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro giuridico e istituzionale frammentato; autorità e capacità cyber ancora deboli, con forte esposizione alla continuità e alla sicurezza fisica.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,5	Crimini finanziari	7,0
Reti criminali	7,5	Attori incorporati nello Stato	8,0
Attori stranieri	6,0	Attori del settore privato	6,5
Resilienza complessiva	1,9	Cooperazione internazionale	3,0
Politiche e norme nazionali	2,5	Forze dell'ordine	1,5
Antiriciclaggio	2,0	Prevenzione	1,5
Supporto vittime e testimoni	1,5	Rischio operativo FOTR-CY	6,2 - SIGNIFICATIVO

Quadro criminale digitale. Per Somalia, l'indice operativo FOTR-CY è 6,2/10, classe significativa. Il mercato dei reati cyber-dipendenti è limitato o poco osservabile (2,5/10), mentre i crimini finanziari sono elevati (7,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e reti criminali (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Somalia assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Somalia, la resilienza complessiva è molto debole (1,9/10); la cooperazione internazionale è molto debole (3,0/10), le politiche e norme nazionali sono molto deboli (2,5/10) e la capacità delle forze dell'ordine è molto debole (1,5/10). Completano il quadro antiriciclaggio 2,0/10, prevenzione 1,5/10 e supporto a vittime e testimoni 1,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Somalia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Somalia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Somalia, In Somalia le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. Per

i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Somalia, Il livello governativo di Somalia presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Somalia, Sul piano militare e dual-use, Somalia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Somalia, Quadro giuridico e istituzionale frammentato; autorità e capacità cyber ancora deboli, con forte esposizione alla continuità e alla sicurezza fisica. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Somalia, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 0,7/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
1,6	2,1	1,0	2,6	1,8	1,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
2,3	0,6	0,8	2,7	0,4	0,7

Il GCRI di Somalia è 1,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 1,3/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (2,7/10), mentre il più basso è Supply chain (0,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 1,3/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Somalia, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Somalia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Somalia, Dal punto di vista italiano, Somalia rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Somalia, il FOTR di 1,3/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

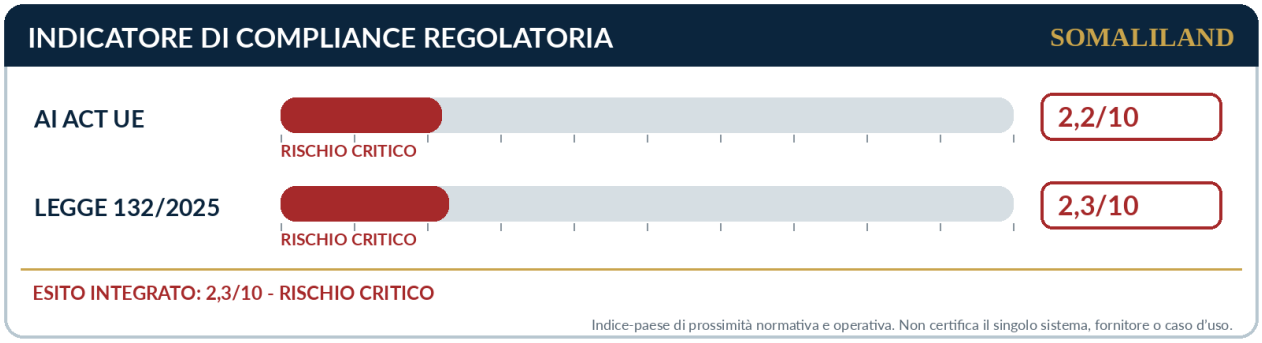
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Somalia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Somaliland

Posizione FOTR	189	Area	Africa	Subregione	Corno d'Africa
Status	Entità de facto priva di riconoscimento internazionale generale	Confidenza Celeborn Intelligence	Bassa	Copertura dati	1/7 famiglie
FOTR / 10	2,2	GCRI / 10	2,2	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Somaliland, AI Act UE 2,2/10; legge 132/2025 2,3/10; esito integrato 2,3/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Somaliland, situato in Corno d'Africa, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Golfo. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 47/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (2,2/10) e indice FOTR (2,2/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Amministrazione de facto relativamente stabile rispetto al contesto somalo, ma senza riconoscimento generale e con capacità infrastrutturali e giuridiche limitate.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	n.d. / n.d. per 100	n.d./n.d.	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	n.d. / n.d. per milione	n.d./n.d.	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	n.d. / n.d.	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	n.d./100 - n.d.	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	21,5/100 - rank 164	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (47/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,1 / 3,0 / 6,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Somaliland, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 1/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Somaliland le evidenze principali sono AI readiness 21,5/100. La dimensione più robusta è indipendenza della supply chain (3,0/10), mentre la criticità relativa riguarda postura di sicurezza cyber (1,7/10). Sono disponibili 1 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata bassa. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Somaliland è 1,9/10. La base statistica rileva i principali dati WDI non sono disponibili in forma omogenea. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Somaliland al posto 164 con un valore medio di 21,5/100; il pilastro migliore è resilienza (29,9/100), quello più debole è adozione pubblica (11,2/100). Il punteggio S2 è 2,2/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Somaliland è valutata fragile, con S3 pari a 2,2/10. Le evidenze disponibili comprendono sviluppo e diffusione dell'IA 22,3/100. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Somaliland ottiene S4 3,0/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Golfo; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Somaliland, Fornitura regionale, del Golfo e asiatica, con infrastrutture di piccola scala e limitata trasparenza. L'impatto sulla valutazione è misurato da S4=3,0/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Somaliland è S5 1,7/10. La base ITU registra GCI non disponibile in forma comparabile. Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (47/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,1	Crimini finanziari	6,9
Reti criminali	7,1	Attori incorporati nello Stato	7,1
Attori stranieri	6,2	Attori del settore privato	6,4
Resilienza complessiva	3,0	Cooperazione internazionale	4,3
Politiche e norme nazionali	3,8	Forze dell'ordine	2,6
Antiriciclaggio	3,6	Prevenzione	2,9
Supporto vittime e testimoni	2,1	Rischio operativo FOTR-CY	6,1 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Somaliland il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 6,1/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 3,1/10; le frodi e i reati finanziari 6,9/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,1/10) e reti criminali (7,1/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Somaliland assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Somaliland, la resilienza complessiva è molto debole (3,0/10); la cooperazione internazionale è debole (4,3/10), le politiche e norme nazionali sono deboli (3,8/10) e la capacità delle forze dell'ordine è molto debole (2,6/10). Completano il quadro antiriciclaggio 3,6/10, prevenzione 2,9/10 e supporto a vittime e testimoni 2,1/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Somaliland, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio. Poiché l'entità non dispone di una serie nazionale GI-TOC autonoma, i valori derivano da un proxy Celeborn Intelligence ponderato su Somalia 55%, Etiopia 25%, Gibuti 20%; la confidenza deve pertanto essere considerata inferiore e la decisione resa più prudente.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; proxy Celeborn Intelligence ponderato su Somalia 55%, Etiopia 25%, Gibuti 20%. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Somaliland, In Somaliland le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Somaliland, Il livello governativo di Somaliland presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Somaliland, Sul piano militare e dual-use, Somaliland mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Somaliland, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Somaliland, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 1,8/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
1,9	2,2	2,2	3,0	1,7	2,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
2,8	1,7	1,7	3,5	1,7	1,8

Il GCRI di Somaliland è 2,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 2,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (3,5/10), mentre il più basso è Maturità cyber (1,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 2,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Somaliland, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Somaliland, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Somaliland, Dal punto di vista italiano, Somaliland rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Somaliland, il FOTR di 2,2/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

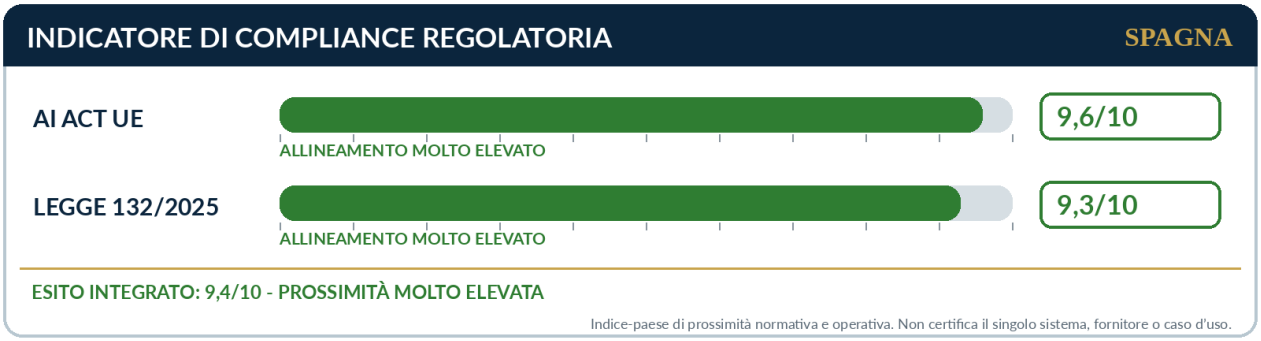
Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.
Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.
Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Somaliland: World Development Indicators, valori più recenti disponibili 2022-2024; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Bassa con copertura 1/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Spagna

Posizione FOTR	24	Area	Europa	Subregione	Europa meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,6	GCRI / 10	8,3	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Spagna, AI Act UE 9,6/10; legge 132/2025 9,3/10; esito integrato 9,4/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Per un operatore italiano, Spagna non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 91/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,3/10) e indice FOTR (8,6/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Spagna presenta un ecosistema digitale maturo, istituzioni generalmente prevedibili e una buona capacità di gestione degli incidenti. Il rischio residuo deriva soprattutto dalla concentrazione cloud, dalle dipendenze extraeuropee e dalla complessità delle filiere software.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	95,8% / 39,2 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 29.986 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	92,1 / 89,1	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	99,7/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	77,9/100 - rank 13	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (91/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,5 / 6,7 / 5,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Spagna, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Spagna le evidenze principali sono GTMI 89,1/100, EGDI 92,1/100, GCI 99,7/100, AI readiness 77,9/100. La dimensione più robusta è maturità infrastrutturale (9,6/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,3/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Spagna è 9,6/10. La base statistica rileva utenti Internet pari al 95,8% nel 2024; 39,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 29.986 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Spagna al posto 13 con un valore medio di 77,9/100; il pilastro migliore è politiche pubbliche (92,0/100), quello più debole è sviluppo e diffusione (62,0/100). Il GTMI 2025 è 89,1/100. Il punteggio S2 è 8,0/10 e indica una capacità elevata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Spagna è valutata solida, con S3 pari a 8,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 89,6/100, sviluppo e diffusione dell'IA 62,0/100, penetrazione Internet 95,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Spagna ottiene S4 6,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Spagna, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Spagna è S5 9,3/10. La base ITU registra ITU GCI 99,7/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è sviluppo delle capacità (19,7/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (91/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, Ley Orgánica 3/2018, Esquema Nacional de Seguridad e disciplina NIS2; piena applicazione dei regolamenti digitali UE.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,5	Crimini finanziari	7,0
Reti criminali	7,0	Attori incorporati nello Stato	5,5
Attori stranieri	7,5	Attori del settore privato	5,0
Resilienza complessiva	6,7	Cooperazione internazionale	8,5
Politiche e norme nazionali	8,0	Forze dell'ordine	8,0
Antiriciclaggio	6,0	Prevenzione	5,5
Supporto vittime e testimoni	6,5	Rischio operativo FOTR-CY	5,8 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Spagna presenta un'esposizione stimata significativa (5,8/10): reati cyber-dipendenti 6,5/10, crimini finanziari 7,0/10 e resilienza 6,7/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (7,5/10) e reti criminali (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Spagna assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Spagna, la resilienza complessiva è intermedia (6,7/10); la cooperazione internazionale è robusta (8,5/10), le politiche e norme nazionali sono robuste (8,0/10) e la capacità delle forze dell'ordine è robusta (8,0/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 5,5/10 e supporto a vittime e testimoni 6,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Spagna, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Spagna. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Spagna, In Spagna le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Spagna, Il livello governativo di Spagna presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Spagna, Sul piano militare e dual-use, Spagna mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Spagna, GDPR, Ley Orgánica 3/2018, Esquema Nacional de Seguridad e disciplina NIS2; piena applicazione dei regolamenti digitali UE. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Spagna, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,7/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,6	8,0	8,1	6,3	9,3	8,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,3	8,2	7,6	9,3	7,5	9,7

Il GCRI di Spagna è 8,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,7/10), mentre il più basso è Supply chain (7,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Spagna, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Spagna, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Spagna, Dal punto di vista italiano, Spagna rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Spagna, il FOTR di 8,6/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Supply chain (7,5/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

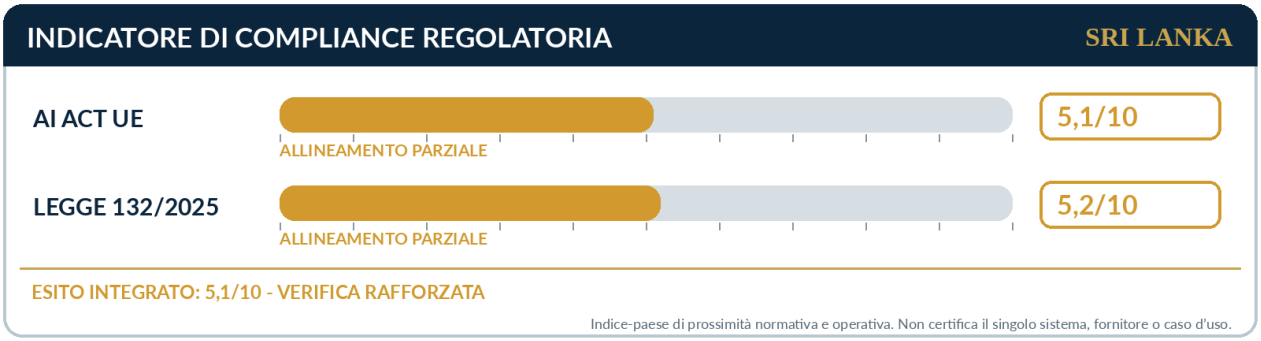
Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Spagna: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Sri Lanka

Posizione FOTR	134	Area	Asia	Subregione	Asia meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,1	GCRI / 10	5,9	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Sri Lanka, AI Act UE 5,1/10; legge 132/2025 5,2/10; esito integrato 5,1/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Sri Lanka è stato membro delle nazioni unite collocato in Asia meridionale. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 63/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,9/10) e indice FOTR (5,1/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Sri Lanka presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	54,6% / 8,5 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 449 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	66,7 / 65,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	87,0/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	48,3/100 - rank 80	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	53/100 - Parzialmente libero / Parzialmente libero (63/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,5 / 3,7 / 4,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Sri Lanka, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Sri Lanka le evidenze principali sono GTMI 65,7/100, EGDI 66,7/100, GCI 87,0/100, AI readiness 48,3/100. La dimensione più robusta è postura di sicurezza cyber (7,0/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (5,2/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Sri Lanka è 6,2/10. La base statistica rileva utenti Internet pari al 54,6% nel 2024; 8,5 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 449 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Sri Lanka al posto 80 con un valore medio di 48,3/100; il pilastro migliore è politiche pubbliche (72,5/100), quello più debole è sviluppo e diffusione (33,3/100). Il GTMI 2025 è 65,7/100. Il punteggio S2 è 5,2/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Sri Lanka è valutata sufficiente ma disomogenea, con S3 pari a 5,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 65,7/100, sviluppo e diffusione dell'IA 33,3/100, penetrazione Internet 54,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Sri Lanka ottiene S4 5,9/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Sri Lanka, Mercato multi-fornitore con influenza cinese, indiana, europea e statunitense. L'impatto sulla valutazione è misurato da S4=5,9/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Sri Lanka è S5 7,0/10. La base ITU registra ITU GCI 87,0/100, Tier 2 - avanzato; il pilastro relativamente più debole è cooperazione (14,3/20). Freedom on the Net è 53/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (63/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,5	Crimini finanziari	4,5
Reti criminali	6,0	Attori incorporati nello Stato	7,0
Attori stranieri	3,5	Attori del settore privato	3,5
Resilienza complessiva	3,7	Cooperazione internazionale	5,5
Politiche e norme nazionali	5,5	Forze dell'ordine	3,5
Antiriciclaggio	5,0	Prevenzione	2,0
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	4,9 - MODERATO

Rischio criminale connesso alle tecnologie. In Sri Lanka il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 4,9/10, livello moderato. I reati che dipendono direttamente da sistemi informatici raggiungono 3,5/10; le frodi e i reati finanziari 4,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,0/10) e reti criminali (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Sri Lanka assumono particolare rilevanza compromissione delle caselle di posta aziendale, frodi da call center, abuso di portafogli digitali mobili, identità sintetiche, ransomware, phishing bancario e triangolazioni transfrontaliere dei proventi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Sri Lanka, la resilienza complessiva è debole (3,7/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è debole (3,5/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 2,0/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Sri Lanka, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Sri Lanka. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Sri Lanka, In Sri Lanka le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Sri Lanka, Il livello governativo di Sri Lanka presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Sri Lanka, Sul piano militare e dual-use, Sri Lanka mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Sri Lanka, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Sri Lanka, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,7/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,2	5,2	5,4	5,9	7,0	5,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,2	5,6	4,7	5,2	5,4	4,7

Il GCRI di Sri Lanka è 5,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,1/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (5,6/10), mentre il più basso è Trasparenza istituzionale (4,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 5,1/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Sri Lanka, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Sri Lanka, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Sri Lanka, Dal punto di vista italiano, Sri Lanka rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Sri Lanka è indicata una cooperazione selettiva, coerente con il FOTR di 5,1/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.
Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

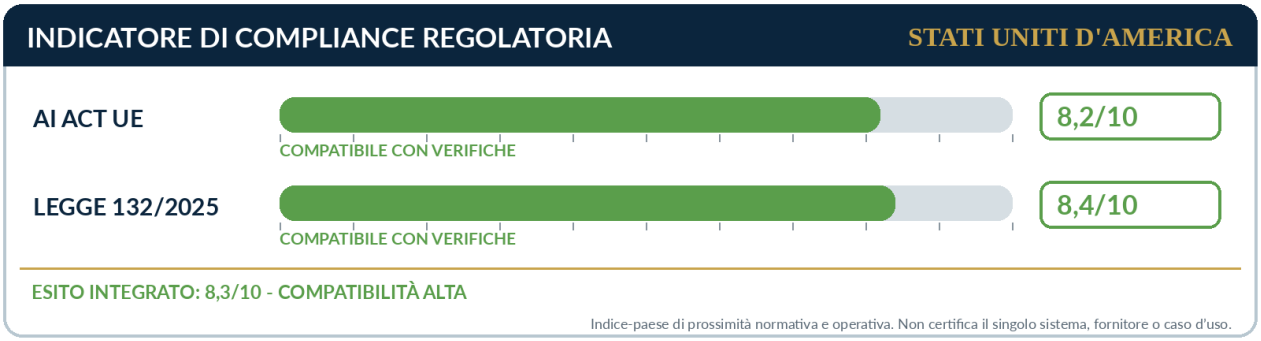
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Sri Lanka: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Stati Uniti d'America

Posizione FOTR	31	Area	Americhe	Subregione	Nord America e Artico
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	8,3	GCRI / 10	8,8	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Stati Uniti d'America, AI Act UE 8,2/10; legge 132/2025 8,4/10; esito integrato 8,3/10, classe «Compatibile con verifiche». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Prima dell'ingaggio occorre una analisi degli scostamenti mirata su trasparenza, governance dei dati, rappresentanza nell'UE, audit e rimedi contrattuali.

Premessa geopolitica e tecnologica

Gli Stati Uniti restano il principale polo occidentale per cloud, software, semiconduttori, cybersicurezza, modelli di intelligenza artificiale e infrastrutture digitali. La cooperazione con l'Italia è sostenuta da NATO, relazioni industriali e meccanismi transatlantici, ma deve essere letta insieme alla concentrazione degli hyperscaler, ai poteri di accesso delle autorità e alla natura condizionata del Data Privacy Framework, applicabile alle sole organizzazioni aderenti. L'elevata affidabilità non elimina quindi il bisogno di crittografia, controllo delle chiavi, portabilità e verifica delle catene societarie. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 81/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,8/10) e indice FOTR (8,3/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Potenza tecnologica di riferimento per cloud, semiconduttori, software, IA e difesa digitale; il valore industriale convive con un regime privacy frammentato e con poteri di accesso governativo da valutare per ogni trasferimento.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	94,7% / 38,9 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 196.616 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	91,9 / 77,1	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	99,9/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	87,7/100 - rank 1	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	73/100 - Libero / Libero (81/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	DPF limitato alle organizzazioni aderenti / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	8,0 / 7,0 / 6,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Stati Uniti d'America, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Stati Uniti d'America le evidenze principali sono GTMI 77,1/100, EGDI 91,9/100, GCI 99,9/100, AI readiness 87,7/100. La dimensione più robusta è maturità infrastrutturale (9,7/10), mentre la criticità relativa riguarda indipendenza della supply chain (8,3/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Stati Uniti d'America è 9,7/10. La base statistica rileva utenti Internet pari al 94,7% nel 2024; 38,9 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 196.616 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Stati Uniti d'America al posto 1 con un valore medio di 87,7/100; il pilastro migliore è adozione pubblica (92,9/100), quello più debole è resilienza (78,3/100). Il GTMI 2025 è 77,1/100. Il punteggio S2 è 8,6/10 e indica una capacità elevata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Stati Uniti d'America è valutata solida, con S3 pari a 8,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 88,4/100, sviluppo e diffusione dell'IA 88,2/100, penetrazione Internet 94,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Stati Uniti d'America ottiene S4 8,3/10 e presenta buona capacità di diversificazione. La provenienza prevalente stimata è Stati Uniti; l'indicatore di indipendenza disponibile è 8,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Stati Uniti d'America, Fornitura prevalentemente domestica per cloud, software, semiconduttori avanzati e difesa; catene hardware globali con forte integrazione asiatica. L'impatto sulla valutazione

è misurato da S4=8,3/10 e dal proxy di indipendenza 8,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Stati Uniti d'America è S5 9,0/10. La base ITU registra ITU GCI 99,9/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è sviluppo delle capacità (19,9/20). Freedom on the Net è 73/100 - Libero, mentre Freedom in the World è Libero (81/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Sistema federale e statale settoriale: FTC Act, HIPAA, GLBA, COPPA, leggi statali sulla privacy; FISA, CLOUD Act e regimi di accesso governativo; trasferimenti UE agevolati solo per organizzazioni aderenti al Data Privacy Framework o con altre garanzie valide.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	8,0	Crimini finanziari	8,0
Reti criminali	6,0	Attori incorporati nello Stato	4,5
Attori stranieri	6,0	Attori del settore privato	6,0
Resilienza complessiva	7,0	Cooperazione internazionale	8,5
Politiche e norme nazionali	6,5	Forze dell'ordine	8,0
Antiriciclaggio	6,0	Prevenzione	7,0
Supporto vittime e testimoni	7,5	Rischio operativo FOTR-CY	6,0 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Stati Uniti d'America restituisce un rischio FOTR-CY di 6,0/10 (significativo). La componente cyber-dipendente vale 8,0/10 e quella finanziaria 8,0/10; la risposta sistemica è valutata intermedia, con resilienza media di 7,0/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (6,0/10) e attori stranieri (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Stati Uniti d'America assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, compromissione della supply chain, compromissione delle caselle di posta aziendale, furto d'identità, abuso di servizi cloud e riciclaggio digitale; l'elevata capacità di denuncia aumenta la visibilità statistica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Stati Uniti d'America, la resilienza complessiva è intermedia (7,0/10); la cooperazione internazionale è robusta (8,5/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è robusta (8,0/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 7,0/10 e supporto a vittime e testimoni 7,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Stati Uniti d'America, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Stati Uniti d'America. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Stati Uniti d'America, In Stati Uniti d'America le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o

nazionali. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Stati Uniti d'America, Il livello governativo di Stati Uniti d'America presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Stati Uniti d'America, Sul piano militare e dual-use, Stati Uniti d'America mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Stati Uniti d'America, Sistema federale e statale settoriale: FTC Act, HIPAA, GLBA, COPPA, leggi statali sulla privacy; FISA, CLOUD Act e regimi di accesso governativo; trasferimenti UE agevolati solo per organizzazioni aderenti al Data Privacy Framework o con altre garanzie valide. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Stati Uniti d'America, Il trasferimento può avvenire verso organizzazioni statunitensi effettivamente certificate nel Data Privacy Framework; negli altri casi servono SCC/BCR o altra base valida, con Transfer Impact Assessment e verifica dei poteri di accesso pubblico. La componente FOTR di trasferibilità è 8,6/10 e il rischio sui dati personali è Medio-basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,7	8,6	8,4	8,3	9,0	8,8

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
7,4	9,5	6,8	9,9	8,2	8,6

Il GCRI di Stati Uniti d'America è 8,8/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,3/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (9,9/10), mentre il più basso è Trasparenza istituzionale (6,8/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-basso	Medio-basso	Basso	Medio-basso	Basso	Medio-basso

La matrice applica il FOTR di 8,3/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Stati Uniti d'America, la cautela si concentra su 4 ambiti a rischio intermedio: Dati personali, Sanità e biometria, IP e R&S, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Stati Uniti d'America, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Stati Uniti d'America, Dal punto di vista italiano, Stati Uniti d'America rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Stati Uniti d'America, il FOTR di 8,3/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (6,8/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

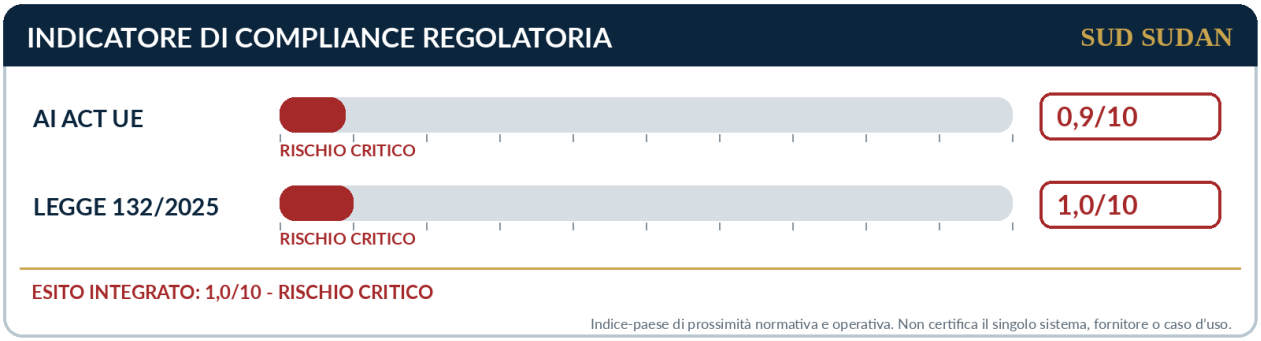
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Stati Uniti d'America: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Sud Sudan

Posizione FOTR	205	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	0,8	GCRI / 10	1,3	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Sud Sudan, AI Act UE 0,9/10; legge 132/2025 1,0/10; esito integrato 1,0/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Sud Sudan, situato in Africa orientale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 0/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (1,3/10) e indice FOTR (0,8/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Sud Sudan ricade nella fascia di rischio estremo. L'assenza di rimedi affidabili, le restrizioni, l'instabilità o le sanzioni rendono normalmente incompatibile il trattamento locale di dati italiani sensibili o strategici.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	6,7% / 0,0 per 100	2019/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	5,4% / 5 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	11,9 / 16,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	34,4/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	10,8/100 - rank 194	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (0/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 2,0 / 6,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Sud Sudan, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Sud Sudan le evidenze principali sono GTMI 16,3/100, EGDI 11,9/100, GCI 34,4/100, AI readiness 10,8/100. La dimensione più robusta è indipendenza della supply chain (2,5/10), mentre la criticità relativa riguarda maturità infrastrutturale (0,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Sud Sudan è 0,1/10. La base statistica rileva utenti Internet pari al 6,7% nel 2019; 0,0 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 5,4% nel 2024; 5 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Sud Sudan al posto 194 con un valore medio di 10,8/100; il pilastro migliore è infrastrutture IA (24,4/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 16,3/100. Il punteggio S2 è 1,4/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Sud Sudan è valutata fragile, con S3 pari a 1,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 15,2/100, sviluppo e diffusione dell'IA 11,4/100, penetrazione Internet 6,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Sud Sudan ottiene S4 2,5/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Sud Sudan, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre

ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=2,5/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Sud Sudan è S5 1,5/10. La base ITU registra ITU GCI 34,4/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è sviluppo delle capacità (1,3/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (0/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo e capacità cyber embrionali; elevatissimi rischi di continuità, sicurezza fisica, rimedi e catena di fornitura.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	7,5
Reti criminali	7,5	Attori incorporati nello Stato	9,0
Attori stranieri	8,0	Attori del settore privato	7,5
Resilienza complessiva	2,0	Cooperazione internazionale	3,0
Politiche e norme nazionali	3,0	Forze dell'ordine	2,0
Antiriciclaggio	1,5	Prevenzione	1,5
Supporto vittime e testimoni	1,5	Rischio operativo FOTR-CY	6,4 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Sud Sudan presenta un'esposizione stimata significativa (6,4/10): reati cyber-dipendenti 2,0/10, crimini finanziari 7,5/10 e resilienza 2,0/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e attori stranieri (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Sud Sudan assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Sud Sudan, la resilienza complessiva è molto debole (2,0/10); la cooperazione internazionale è molto debole (3,0/10), le politiche e norme nazionali sono molto deboli (3,0/10) e la capacità delle forze dell'ordine è molto debole (2,0/10). Completano il quadro antiriciclaggio 1,5/10, prevenzione 1,5/10 e supporto a vittime e testimoni 1,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Sud Sudan, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Sud Sudan. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Sud Sudan, In Sud Sudan le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture

esterne. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Sud Sudan, Il livello governativo di Sud Sudan presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Sud Sudan, Sul piano militare e dual-use, Sud Sudan mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Sud Sudan, Quadro normativo e capacità cyber embrionali; elevatissimi rischi di continuità, sicurezza fisica, rimedi e catena di fornitura. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Sud Sudan, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 0,4/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
0,1	1,4	1,1	2,5	1,5	1,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
1,4	0,2	0,5	2,1	0,5	0,4

Il GCRI di Sud Sudan è 1,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 0,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (2,1/10), mentre il più basso è Maturità cyber (0,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 0,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Sud Sudan, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Sud Sudan, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Sud Sudan, Dal punto di vista italiano, Sud Sudan rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Sud Sudan, il FOTR di 0,8/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

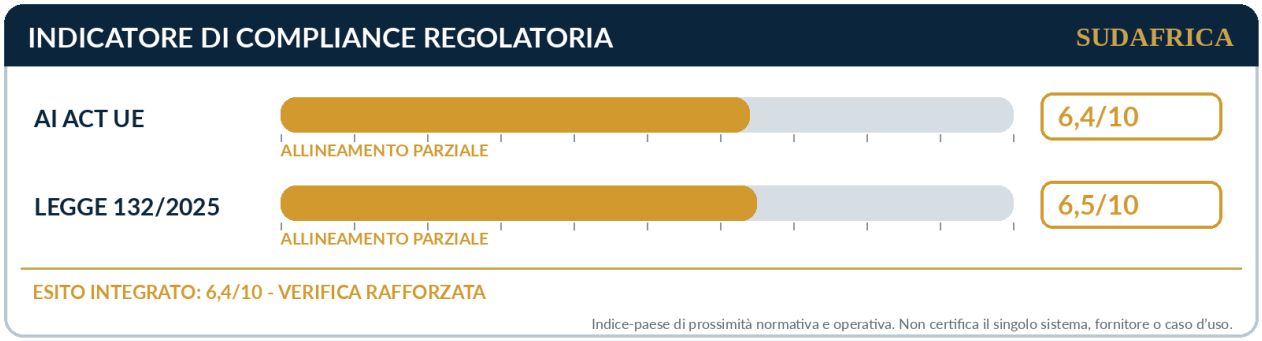
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Sud Sudan: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Sudafrica

Posizione FOTR	60	Area	Africa	Subregione	Africa australe
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	6,4	GCRI / 10	6,6	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Sudafrica, AI Act UE 6,4/10; legge 132/2025 6,5/10; esito integrato 6,4/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Sudafrica non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La partecipazione al coordinamento BRICS segnala una strategia di autonomia e diversificazione rispetto agli ecosistemi occidentali, con relazioni tecnologiche più intense verso Cina, Russia o altri poli emergenti. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 81/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,6/10) e indice FOTR (6,4/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Il quadro di Sudafrica è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	78,4% / 5,3 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	90,2% / 16.658 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	86,2 / 62,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	72,7/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	53,8/100 - rank 65	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	73/100 - Libero / Libero (81/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Firmatario/invitato	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	8,0 / 5,7 / 7,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Sudafrica, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Sudafrica le evidenze principali sono GTMI 62,3/100, EGDI 86,2/100, GCI 72,7/100, AI readiness 53,8/100. La dimensione più robusta è maturità infrastrutturale (7,3/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (6,0/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Sudafrica è 7,3/10. La base statistica rileva utenti Internet pari al 78,4% nel 2024; 5,3 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 90,2% nel 2024; 16.658 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Sudafrica al posto 65 con un valore medio di 53,8/100; il pilastro migliore è governance (76,6/100), quello più debole è sviluppo e diffusione (37,3/100). Il GTMI 2025 è 62,3/100. Il punteggio S2 è 6,0/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Sudafrica è valutata sufficiente ma disomogenea, con S3 pari a 6,7/10. Le evidenze disponibili comprendono indice UN di capitale umano 80,3/100, sviluppo e diffusione dell'IA 37,3/100, penetrazione Internet 78,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Sudafrica ottiene S4 6,2/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Sudafrica, Mercato multi-fornitore con gruppi europei, statunitensi, cinesi e capacità regionali. L'impatto sulla valutazione è misurato da S4=6,2/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Sudafrica è S5 7,0/10. La base ITU registra ITU GCI 72,7/100, Tier 2 - avanzato; il pilastro relativamente più debole è misure giuridiche (6,5/20). Freedom on the Net è 73/100 - Libero, mentre Freedom in the World è Libero (81/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Firmatario/invitato. Quadro normativo sintetico: Protection of Personal Information Act, Cybercrimes Act e regolazione settoriale; buon impianto formale, con capacità e resilienza non uniformi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	8,0	Crimini finanziari	7,5
Reti criminali	8,0	Attori incorporati nello Stato	8,0
Attori stranieri	7,5	Attori del settore privato	7,0
Resilienza complessiva	5,7	Cooperazione internazionale	7,0
Politiche e norme nazionali	7,0	Forze dell'ordine	4,5
Antiriciclaggio	5,0	Prevenzione	4,5
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	7,0 - ALTO

Pressione del crimine digitale. Il profilo di Sudafrica restituisce un rischio FOTR-CY di 7,0/10 (alto). La componente cyber-dipendente vale 8,0/10 e quella finanziaria 7,5/10; la risposta sistemica è valutata intermedia, con resilienza media di 5,7/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (8,0/10) e attori incorporati nello Stato (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Sudafrica assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Sudafrica, la resilienza complessiva è intermedia (5,7/10); la cooperazione internazionale è intermedia (7,0/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è debole (4,5/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 4,5/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Sudafrica, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Sudafrica. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Sudafrica, In Sudafrica le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Sudafrica, Il livello governativo di Sudafrica presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Sudafrica, Sul piano militare e dual-use, Sudafrica mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Sudafrica, Protection of Personal Information Act, Cybercrimes Act e regolazione settoriale; buon impianto formale, con capacità e resilienza non uniformi. Lo stato rispetto alla Convenzione di Budapest è: Firmatario/invitato; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Sudafrica, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 6,1/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,3	6,0	6,7	6,2	7,0	6,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,4	6,3	6,5	7,1	6,0	6,1

Il GCRI di Sudafrica è 6,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (7,1/10), mentre il più basso è Supply chain (6,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Sudafrica, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Sudafrica, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Sudafrica, Dal punto di vista italiano, Sudafrica rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Sudafrica è indicata una cooperazione selettiva, coerente con il FOTR di 6,4/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Supply chain a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

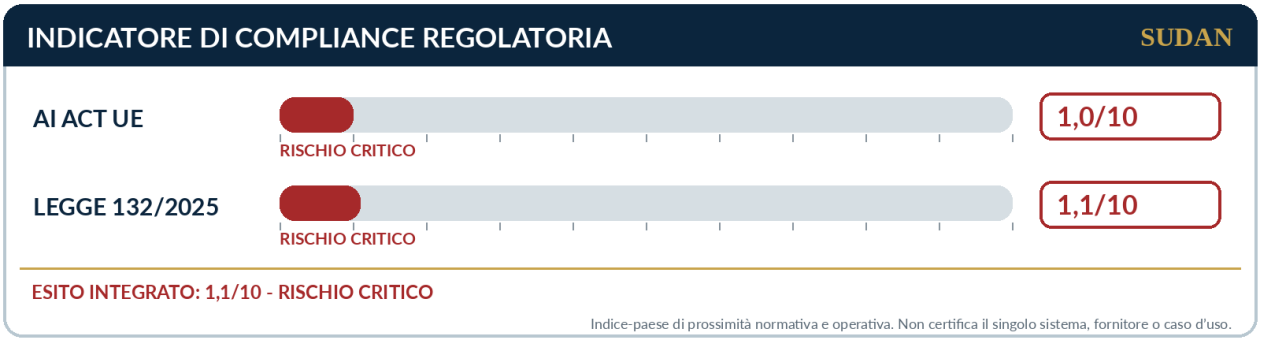
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Sudafrica: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Sudan

Posizione FOTR	204	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	0,9	GCRI / 10	2,2	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Sudan, AI Act UE 1,0/10; legge 132/2025 1,1/10; esito integrato 1,1/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Sudan è stato membro delle nazioni unite collocato in Africa orientale. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 1/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (2,2/10) è superiore al punteggio FOTR (0,9/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Il rapporto digitale con Sudan deve essere considerato eccezionale e ad alta esposizione. Sono necessari screening sanzionatori, autorizzazioni, segregazione completa e impossibilità tecnica di accedere ai dati in chiaro.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	18,6% / 0,1 per 100	2017/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	66,0% / 2 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	27,6 / 14,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	48,2/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	15,2/100 - rank 186	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	27/100 - Non libero / Non libero (1/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 2,2 / 6,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Sudan, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Sudan le evidenze principali sono GTMI 14,3/100, EGDI 27,6/100, GCI 48,2/100, AI readiness 15,2/100. La dimensione più robusta è indipendenza della supply chain (2,7/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (1,6/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Sudan è 2,4/10. La base statistica rileva utenti Internet pari al 18,6% nel 2017; 0,1 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 66,0% nel 2024; 2 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Sudan al posto 186 con un valore medio di 15,2/100; il pilastro migliore è infrastrutture IA (24,5/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 14,3/100. Il punteggio S2 è 1,6/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Sudan è valutata fragile, con S3 pari a 1,8/10. Le evidenze disponibili comprendono indice UN di capitale umano 25,9/100, sviluppo e diffusione dell'IA 12,0/100, penetrazione Internet 18,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Sudan ottiene S4 2,7/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Sudan, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=2,7/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Sudan è S5 2,3/10. La base ITU registra ITU GCI 48,2/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è sviluppo delle capacità (4,4/20). Freedom on the Net è 27/100 - Non libero, mentre Freedom in the World è Non libero (1/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Disciplina cyber e telecomunicazioni in un contesto istituzionale e di sicurezza gravemente instabile; trasferimenti strategici da evitare salvo eccezioni protette.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	7,5
Reti criminali	6,5	Attori incorporati nello Stato	8,5
Attori stranieri	8,0	Attori del settore privato	7,5
Resilienza complessiva	2,2	Cooperazione internazionale	4,0
Politiche e norme nazionali	4,5	Forze dell'ordine	2,0
Antiriciclaggio	3,0	Prevenzione	1,5
Supporto vittime e testimoni	1,0	Rischio operativo FOTR-CY	6,5 - ALTO

Quadro criminale digitale. Per Sudan, l'indice operativo FOTR-CY è 6,5/10, classe alta. Il mercato dei reati cyber-dipendenti è limitato o poco osservabile (3,0/10), mentre i crimini finanziari sono molto elevati (7,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,5/10) e attori stranieri (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Sudan assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Sudan, la resilienza complessiva è molto debole (2,2/10); la cooperazione internazionale è debole (4,0/10), le politiche e norme nazionali sono deboli (4,5/10) e la capacità delle forze dell'ordine è molto debole (2,0/10). Completano il quadro antiriciclaggio 3,0/10, prevenzione 1,5/10 e supporto a vittime e testimoni 1,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Sudan, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Sudan. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Sudan, In Sudan le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. La

disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Sudan, Il livello governativo di Sudan presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Sudan, Sul piano militare e dual-use, Sudan mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Sudan, Disciplina cyber e telecomunicazioni in un contesto istituzionale e di sicurezza gravemente instabile; trasferimenti strategici da evitare salvo eccezioni protette. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Sudan, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 0,1/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
2,4	1,6	1,8	2,7	2,3	2,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
1,7	0,3	0,7	2,0	0,6	0,1

Il GCRI di Sudan è 2,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 0,9/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (2,0/10), mentre il più basso è Trasferibilità dati (0,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 0,9/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Sudan, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Sudan, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Sudan, Dal punto di vista italiano, Sudan rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Sudan, il FOTR di 0,9/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

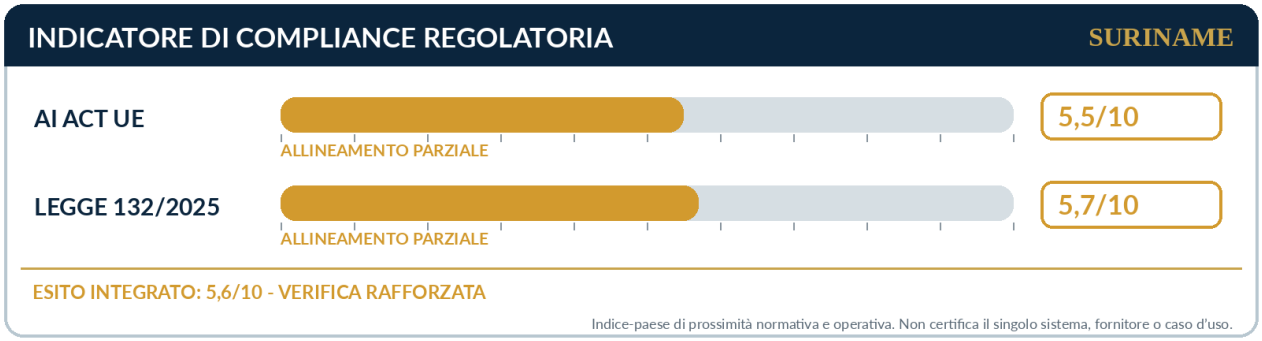
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Sudan: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Suriname

Posizione FOTR	**91**	**Area**	Americhe	**Subregione**	America meridionale
Status	**Stato membro delle Nazioni Unite**	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	**5,8**	**GCRI / 10**	**4,7**	**Classe operativa**	**Affidabilità selettiva**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Suriname, AI Act UE 5,5/10; legge 132/2025 5,7/10; esito integrato 5,6/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Americhe, Suriname presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 81/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,8/10) supera il GCRI tecnico (4,7/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Suriname dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	87,4% / 18,8 per 100	2023/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	99,0% / 2.060 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	63,7 / 32,5	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	34,8/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	16,2/100 - rank 181	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (81/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,0 / 3,2 / 5,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Suriname, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Suriname le evidenze principali sono GTMI 32,5/100, EGDI 63,7/100, GCI 34,8/100, AI readiness 16,2/100. La dimensione più robusta è maturità infrastrutturale (7,9/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,5/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Suriname è 7,9/10. La base statistica rileva utenti Internet pari al 87,4% nel 2023; 18,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 99,0% nel 2024; 2.060 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Suriname al posto 181 con un valore medio di 16,2/100; il pilastro migliore è infrastrutture IA (34,9/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 32,5/100. Il punteggio S2 è 2,5/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Suriname è valutata fragile, con S3 pari a 4,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 55,7/100, sviluppo e diffusione dell'IA 13,6/100, penetrazione Internet 87,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Suriname ottiene S4 4,9/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Suriname, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=4,9/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Suriname è S5 4,3/10. La base ITU registra ITU GCI 34,8/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è sviluppo delle capacità (2,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (81/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,0	Crimini finanziari	5,0
Reti criminali	5,0	Attori incorporati nello Stato	8,5
Attori stranieri	6,0	Attori del settore privato	4,0
Resilienza complessiva	3,2	Cooperazione internazionale	5,0
Politiche e norme nazionali	3,0	Forze dell'ordine	3,0
Antiriciclaggio	2,5	Prevenzione	4,5
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	5,6 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Suriname il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,6/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 4,0/10; le frodi e i reati finanziari 5,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,5/10) e attori stranieri (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Suriname assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Suriname, la resilienza complessiva è molto debole (3,2/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono molto deboli (3,0/10) e la capacità delle forze dell'ordine è molto debole (3,0/10). Completano il quadro antiriciclaggio 2,5/10, prevenzione 4,5/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Suriname, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Suriname. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Suriname, In Suriname le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio

comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Suriname, Il livello governativo di Suriname presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Suriname, Sul piano militare e dual-use, Suriname mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Suriname, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Suriname, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,4/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,9	2,5	4,1	4,9	4,3	4,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,9	5,9	5,9	5,9	5,6	5,4

Il GCRI di Suriname è 4,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,8/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (5,9/10), mentre il più basso è Trasferibilità dati (5,4/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,8/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Suriname, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Suriname, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Suriname, Dal punto di vista italiano, Suriname rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Suriname è indicata una cooperazione selettiva, coerente con il FOTR di 5,8/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasferibilità dati a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

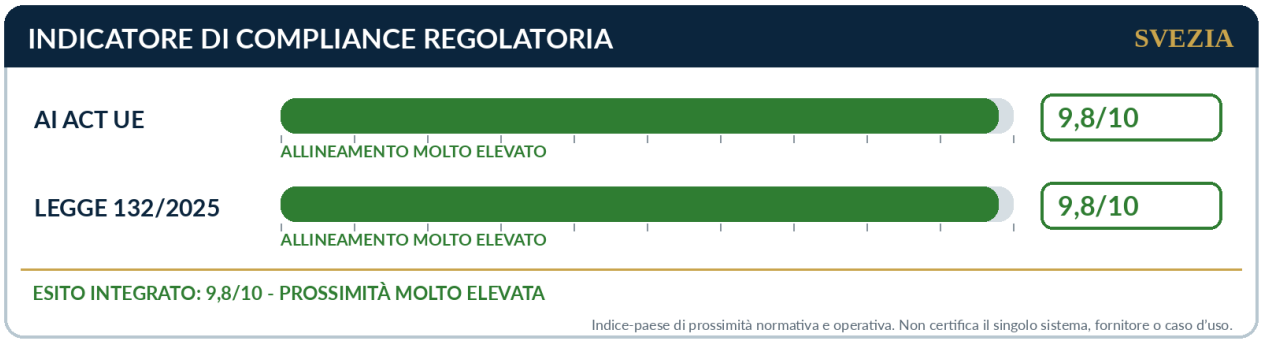
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Suriname: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Svezia

Posizione FOTR	5	**Area**	Europa	**Subregione**	Europa settentrionale e baltica
Status	Stato membro delle Nazioni Unite	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	**9,3**	**GCRI / 10**	**8,3**	**Classe operativa**	**Affidabilità molto alta**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Svezia, AI Act UE 9,8/10; legge 132/2025 9,8/10; esito integrato 9,8/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Svezia, situato in Europa settentrionale e baltica, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 99/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (9,3/10) supera il GCRI tecnico (8,3/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il sistema digitale di Svezia è avanzato e integrato con standard internazionali. Le principali criticità non sono di base istituzionale, ma riguardano supply chain, concentrazione dei servizi e gestione delle eccezioni di sicurezza nazionale.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	95,8% / 40,6 per 100	2025/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 55.097 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	93,3 / 79,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	99,3/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	71,7/100 - rank 23	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (99/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,5 / 7,4 / 5,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Svezia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Svezia le evidenze principali sono GTMI 79,7/100, EGDI 93,3/100, GCI 99,3/100, AI readiness 71,7/100. La dimensione più robusta è maturità infrastrutturale (9,8/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,5/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Svezia è 9,8/10. La base statistica rileva utenti Internet pari al 95,8% nel 2025; 40,6 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 55.097 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Svezia al posto 23 con un valore medio di 71,7/100; il pilastro migliore è politiche pubbliche (89,0/100), quello più debole è sviluppo e diffusione (57,0/100). Il GTMI 2025 è 79,7/100. Il punteggio S2 è 7,5/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Svezia è valutata solida, con S3 pari a 8,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 92,7/100, sviluppo e diffusione dell'IA 57,0/100, penetrazione Internet 95,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Svezia ottiene S4 6,5/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open

source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Svezia, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario, luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,5/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Svezia è S5 9,5/10. La base ITU registra ITU GCI 99,3/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è organizzazione (19,3/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (99/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, Data Protection Act svedese, Protective Security Act e disciplina NIS2; quadro UE integralmente applicabile.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,5	Crimini finanziari	6,5
Reti criminali	6,5	Attori incorporati nello Stato	2,0
Attori stranieri	6,5	Attori del settore privato	3,5
Resilienza complessiva	7,4	Cooperazione internazionale	8,5
Politiche e norme nazionali	8,0	Forze dell'ordine	6,0
Antiriciclaggio	8,0	Prevenzione	7,0
Supporto vittime e testimoni	6,0	Rischio operativo FOTR-CY	5,1 - SIGNIFICATIVO

Quadro criminale digitale. Per Svezia, l'indice operativo FOTR-CY è 5,1/10, classe significativa. Il mercato dei reati cyber-dipendenti è elevato (6,5/10), mentre i crimini finanziari sono elevati (6,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (6,5/10) e attori stranieri (6,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Svezia assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Svezia, la resilienza complessiva è intermedia (7,4/10); la cooperazione internazionale è robusta (8,5/10), le politiche e norme nazionali sono robuste (8,0/10) e la capacità delle forze dell'ordine è intermedia (6,0/10). Completano il quadro antiriciclaggio 8,0/10, prevenzione 7,0/10 e supporto a vittime e testimoni 6,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Svezia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Svezia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Svezia, In Svezia le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Svezia, Il livello governativo di Svezia presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Svezia, Sul piano militare e dual-use, Svezia mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Svezia, GDPR, Data Protection Act svedese, Protective Security Act e disciplina NIS2; quadro UE integralmente applicabile. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Svezia, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 10,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,8	7,5	8,1	6,5	9,5	8,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,9	9,1	8,2	9,9	8,6	10,0

Il GCRI di Svezia è 8,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 9,3/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (10,0/10), mentre il più basso è Trasparenza istituzionale (8,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Basso	Basso	Basso

La matrice applica il FOTR di 9,3/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Svezia, la matrice non individua ambiti ad alto rischio; 6 categorie risultano basse o medio-basse, ferma la verifica del singolo progetto. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Svezia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Svezia, Dal punto di vista italiano, Svezia rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Svezia, il FOTR di 9,3/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (8,2/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

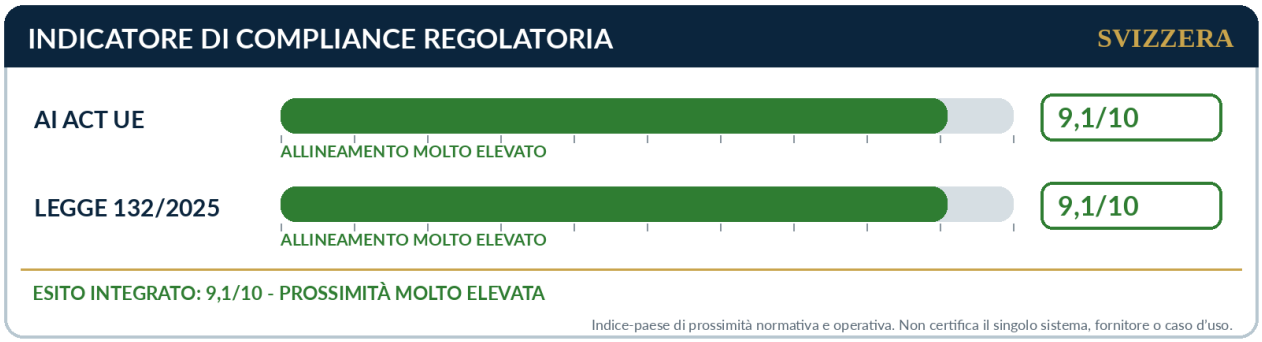
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Svezia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Svizzera

Posizione FOTR	7	**Area**	Europa	**Subregione**	Europa occidentale e centrale
Status	Stato membro delle Nazioni Unite	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	9,2	**GCRI / 10**	8,2	**Classe operativa**	**Affidabilità molto alta**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Svizzera, AI Act UE 9,1/10; legge 132/2025 9,1/10; esito integrato 9,1/10, classe «Allineamento molto elevato». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Per un operatore italiano, Svizzera non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La prossimità europea può ridurre i costi operativi, ma non sostituisce la verifica dell'allineamento al GDPR, delle autorità indipendenti e della reale origine dei servizi cloud. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 96/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (9,2/10) supera il GCRI tecnico (8,2/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Svizzera presenta un ecosistema digitale maturo, istituzioni generalmente prevedibili e una buona capacità di gestione degli incidenti. Il rischio residuo deriva soprattutto dalla concentrazione cloud, dalle dipendenze extraeuropee e dalla complessità delle filiere software.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	97,3% / 47,0 per 100	2025/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 167.358 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	90,0 / 79,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	91,3/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	65,4/100 - rank 26	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (96/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,0 / 7,2 / 5,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Svizzera, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Svizzera le evidenze principali sono GTMI 79,6/100, EGDI 90,0/100, GCI 91,3/100, AI readiness 65,4/100. La dimensione più robusta è maturità infrastrutturale (9,8/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,8/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Svizzera è 9,8/10. La base statistica rileva utenti Internet pari al 97,3% nel 2025; 47,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 167.358 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Svizzera al posto 26 con un valore medio di 65,4/100; il pilastro migliore è governance (89,2/100), quello più debole è politiche pubbliche (39,0/100). Il GTMI 2025 è 79,6/100. Il punteggio S2 è 7,1/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Svizzera è valutata solida, con S3 pari a 8,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 90,3/100, sviluppo e diffusione dell'IA 61,4/100, penetrazione Internet 97,3%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Svizzera ottiene S4 6,8/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open

source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Svizzera, Fornitura prevalentemente nazionale, europea e statunitense, con catene hardware globali. In genere è possibile diversificare e imporre requisiti contrattuali elevati. L'impatto sulla valutazione è misurato da S4=6,8/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Svizzera è S5 9,1/10. La base ITU registra ITU GCI 91,3/100, Tier 2 - avanzato; il pilastro relativamente più debole è cooperazione (15,8/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (96/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge federale sulla protezione dei dati riveduta, ordinanze attuative e disciplina settoriale; decisione UE di adeguatezza e robusto sistema di rimedi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,0	Crimini finanziari	7,5
Reti criminali	3,0	Attori incorporati nello Stato	1,5
Attori stranieri	7,0	Attori del settore privato	7,5
Resilienza complessiva	7,2	Cooperazione internazionale	8,0
Politiche e norme nazionali	7,0	Forze dell'ordine	7,5
Antiriciclaggio	5,5	Prevenzione	6,5
Supporto vittime e testimoni	7,5	Rischio operativo FOTR-CY	5,1 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Svizzera il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,1/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 7,0/10; le frodi e i reati finanziari 7,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori del settore privato (7,5/10) e attori stranieri (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Svizzera assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Svizzera, la resilienza complessiva è intermedia (7,2/10); la cooperazione internazionale è robusta (8,0/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è robusta (7,5/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 6,5/10 e supporto a vittime e testimoni 7,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Svizzera, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Svizzera. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Svizzera, In Svizzera le tecnologie destinate alla popolazione mostrano servizi mobili a larga banda, pagamenti digitali, cloud consumer, identità elettronica e piattaforme con elevata penetrazione. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Svizzera, Il livello governativo di Svizzera presenta servizi pubblici digitali integrati, identità elettronica, interoperabilità e capacità di risposta agli incidenti generalmente mature. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Svizzera, Sul piano militare e dual-use, Svizzera mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Svizzera, Legge federale sulla protezione dei dati riveduta, ordinanze attuative e disciplina settoriale; decisione UE di adeguatezza e robusto sistema di rimedi. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Svizzera, È disponibile una decisione UE di adeguatezza. L'operatore italiano deve comunque controllare la portata della decisione, i trasferimenti successivi, le misure di sicurezza e le eventuali discipline settoriali. La componente FOTR di trasferibilità è 10,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,8	7,1	8,2	6,8	9,1	8,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
9,6	9,5	8,3	8,7	9,3	10,0

Il GCRI di Svizzera è 8,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 9,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (10,0/10), mentre il più basso è Trasparenza istituzionale (8,3/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Basso	Basso	Basso	Basso	Basso

La matrice applica il FOTR di 9,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Svizzera, la matrice non individua ambiti ad alto rischio; 6 categorie risultano basse o medio-basse, ferma la verifica del singolo progetto. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Svizzera, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Svizzera, Dal punto di vista italiano, Svizzera rientra nella classe «Affidabilità molto alta»: cooperazione ordinariamente favorevole, subordinata a verifica preventiva standard elevata, clausole di sicurezza, verifica dei subfornitori e piano di uscita. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Svizzera, il FOTR di 9,2/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (8,3/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

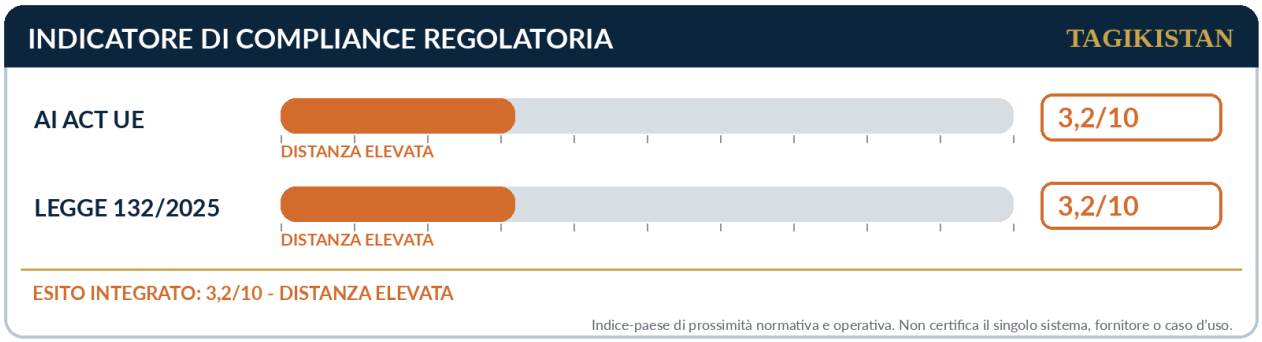
Controllare concentrazione cloud, lock-in e dipendenze extra-SEE anche quando il contratto è europeo.

Profilo Celeborn Intelligence di Svizzera: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Tagikistan

Posizione FOTR	186	Area	Asia	Subregione	Caucaso e Asia centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	3,2	GCRI / 10	3,9	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Tagikistan, AI Act UE 3,2/10; legge 132/2025 3,2/10; esito integrato 3,2/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Tagikistan è stato membro delle nazioni unite collocato in Caucaso e Asia centrale. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina, Russia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 5/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (3,9/10) e indice FOTR (3,2/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Tagikistan presenta un livello di rischio elevato per cooperazione digitale, dovuto a limitata trasparenza, poteri pubblici, instabilità o dipendenze tecnologiche. Le attività dovrebbero escludere dati sensibili e asset strategici.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	55,8% / 1,0 per 100	2024/2023	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	99,9% / 152 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	56,1 / 29,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	25,4/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	32,8/100 - rank 130	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (5/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,0 / 2,5 / 5,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Tagikistan, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Tagikistan le evidenze principali sono GTMI 29,4/100, EGDI 56,1/100, GCI 25,4/100, AI readiness 32,8/100. La dimensione più robusta è maturità infrastrutturale (5,1/10), mentre la criticità relativa riguarda postura di sicurezza cyber (2,8/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Tagikistan è 5,1/10. La base statistica rileva utenti Internet pari al 55,8% nel 2024; 1,0 abbonamenti fissi ogni 100 abitanti nel 2023; accesso all'elettricità del 99,9% nel 2024; 152 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Tagikistan al posto 130 con un valore medio di 32,8/100; il pilastro migliore è politiche pubbliche (54,0/100), quello più debole è infrastrutture IA (20,7/100). Il GTMI 2025 è 29,4/100. Il punteggio S2 è 3,2/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Tagikistan è valutata fragile, con S3 pari a 4,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 65,3/100, sviluppo e diffusione dell'IA 21,2/100, penetrazione Internet 55,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Tagikistan ottiene S4 4,1/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina, Russia; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Tagikistan, Prevalenza cinese e russa nelle reti, nella sicurezza e nelle infrastrutture pubbliche. L'impatto sulla valutazione è misurato da S4=4,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Tagikistan è S5 2,8/10. La base ITU registra ITU GCI 25,4/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (5/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Legge sulla protezione dei dati e ampi controlli pubblici sulle comunicazioni; scarsa trasparenza e capacità limitata.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,0	Crimini finanziari	6,5
Reti criminali	5,0	Attori incorporati nello Stato	9,0
Attori stranieri	5,0	Attori del settore privato	5,0
Resilienza complessiva	2,5	Cooperazione internazionale	3,0
Politiche e norme nazionali	2,0	Forze dell'ordine	3,0
Antiriciclaggio	3,0	Prevenzione	2,5
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	5,5 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Tagikistan restituisce un rischio FOTR-CY di 5,5/10 (significativo). La componente cyber-dipendente vale 2,0/10 e quella finanziaria 6,5/10; la risposta sistemica è valutata molto debole, con resilienza media di 2,5/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e reti criminali (5,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Tagikistan assumono particolare rilevanza ransomware come servizio, malware sottrattori di informazioni, infrastrutture di hosting permissive, DDoS, furto di credenziali, estorsione dei dati e possibili sovrapposizioni tra criminalità professionale e finalità geopolitiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Tagikistan, la resilienza complessiva è molto debole (2,5/10); la cooperazione internazionale è molto debole (3,0/10), le politiche e norme nazionali sono molto deboli (2,0/10) e la capacità delle forze dell'ordine è molto debole (3,0/10). Completano il quadro antiriciclaggio 3,0/10, prevenzione 2,5/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Tagikistan, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Tagikistan. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Tagikistan, In Tagikistan le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. Per

i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Tagikistan, Il livello governativo di Tagikistan presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Tagikistan, Sul piano militare e dual-use, Tagikistan mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Tagikistan, Legge sulla protezione dei dati e ampi controlli pubblici sulle comunicazioni; scarsa trasparenza e capacità limitata. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Tagikistan, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 2,9/10 e il rischio sui dati personali è Alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
5,1	3,2	4,5	4,1	2,8	3,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
3,5	3,6	2,7	2,9	3,5	2,9

Il GCRI di Tagikistan è 3,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 3,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (3,6/10), mentre il più basso è Trasparenza istituzionale (2,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Alto	Alto	Alto	Alto	Alto	Alto

La matrice applica il FOTR di 3,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Tagikistan, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Tagikistan, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Tagikistan, Dal punto di vista italiano, Tagikistan rientra nella classe «Rischio alto»: cooperazione eccezionale e ad alto controllo, subordinata a assenza di dati sensibili, verifica sanzionatoria, autorizzazioni interne e impossibilità di accesso ai sistemi strategici. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Tagikistan, il FOTR di 3,2/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

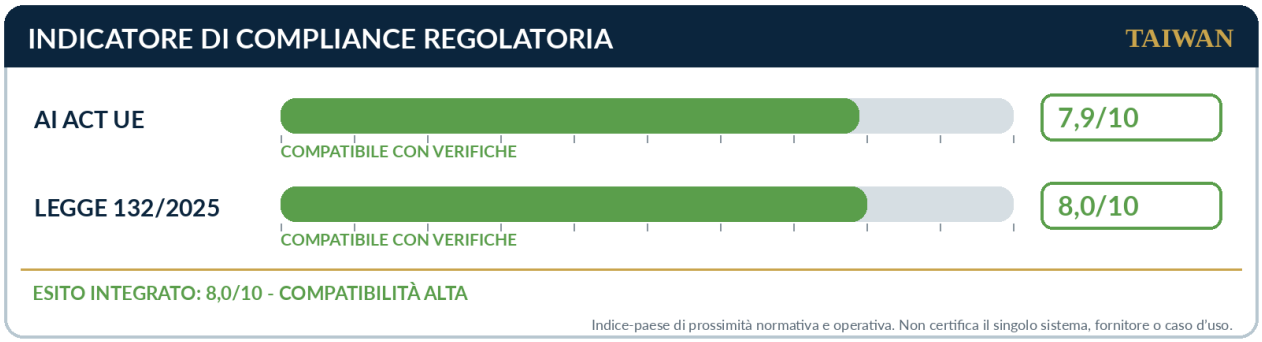
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Tagikistan: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Taiwan

Posizione FOTR	42	**Area**	Asia	**Subregione**	Asia orientale
Status	**Entità a riconoscimento diplomatico limitato e ampia autonomia di fatto**	**Confidenza Celeborn Intelligence**	Bassa	**Copertura dati**	2/7 famiglie
FOTR / 10	**7,9**	**GCRI / 10**	**8,1**	**Classe operativa**	**Affidabilità favorevole ma condizionata**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Taiwan, AI Act UE 7,9/10; legge 132/2025 8,0/10; esito integrato 8,0/10, classe «Compatibile con verifiche». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Prima dell'ingaggio occorre una analisi degli scostamenti mirata su trasparenza, governance dei dati, rappresentanza nell'UE, audit e rimedi contrattuali.

Premessa geopolitica e tecnologica

Taiwan è un nodo indispensabile della filiera globale dei semiconduttori e dell'elettronica avanzata. La qualità industriale, la libertà dell'ecosistema digitale e la cooperazione con Stati Uniti, Giappone ed Europa sono elevate; il principale elemento di rischio non è la maturità tecnica, bensì la continuità geopolitica, logistica ed energetica in uno scenario di pressione militare e diplomatica. Per gli operatori italiani la priorità è progettare ridondanza, scorte, second sourcing e protezione della proprietà intellettuale. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 93/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (8,1/10) e indice FOTR (7,9/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Nodo strategico della filiera mondiale dei semiconduttori e delle tecnologie avanzate; elevata affidabilità industriale, con rischio geopolitico e di continuità da mitigare.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	n.d. / n.d. per 100	n.d./n.d.	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	n.d. / n.d. per milione	n.d./n.d.	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	n.d. / 80,5	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	n.d./100 - n.d.	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Intelligenza artificiale	Government AI Readiness	n.d./100 - rank n.d.	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	79/100 - Libero / Libero (93/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,7 / 7,1 / 5,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Taiwan, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 2/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Taiwan le evidenze principali sono GTMI 80,5/100. La dimensione più robusta è maturità infrastrutturale (8,8/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (7,0/10). Sono disponibili 2 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata bassa. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Taiwan è 8,8/10. La base statistica rileva i principali dati WDI non sono disponibili in forma omogenea. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Per Taiwan non è disponibile un profilo Oxford Insights direttamente attribuibile; l'adozione di IA è quindi valutata attraverso GovTech, servizi online, infrastrutture e fonti qualitative. Il GTMI 2025 è 80,5/100. Il punteggio S2 è 8,1/10 e indica una capacità elevata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Taiwan è valutata sufficiente ma disomogenea, con S3 pari a 7,0/10. Le evidenze disponibili comprendono evidenza quantitativa incompleta. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Taiwan ottiene S4 8,1/10 e presenta buona capacità di diversificazione. La provenienza prevalente stimata è Asia orientale domestica, Italia/UE, Stati Uniti, Giappone/Corea; l'indicatore di indipendenza disponibile è 8,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Taiwan, Fornitura domestica per semiconduttori e hardware avanzato, con strumenti e software statunitensi, europei e giapponesi. L'impatto sulla valutazione è misurato da S4=8,1/10 e dal proxy di indipendenza 8,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Taiwan è S5 8,3/10. La base ITU registra GCI non disponibile in forma comparabile. Freedom on the Net è 79/100 - Libero, mentre Freedom in the World è Libero (93/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Personal Data Protection Act, Cyber Security Management Act e disciplina settoriale; elevata capacità tecnologica, ma assenza di decisione UE di adeguatezza.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,7	Crimini finanziari	6,1
Reti criminali	6,1	Attori incorporati nello Stato	4,2
Attori stranieri	4,4	Attori del settore privato	5,6
Resilienza complessiva	7,1	Cooperazione internazionale	8,1
Politiche e norme nazionali	7,9	Forze dell'ordine	7,2
Antiriciclaggio	7,4	Prevenzione	6,5
Supporto vittime e testimoni	5,6	Rischio operativo FOTR-CY	5,0 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (5,7/10), criminalità finanziaria (6,1/10) e resilienza (7,1/10) colloca Taiwan in una fascia di rischio significativo, pari a 5,0/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (6,1/10) e attori del settore privato (5,6/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Taiwan assumono particolare rilevanza compromissioni della supply chain, sottrazione di proprietà intellettuale, furto di cripto-attività, phishing mirato, abuso di identità digitali e intrusioni persistenti contro industria e amministrazioni. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Taiwan, la resilienza complessiva è intermedia (7,1/10); la cooperazione internazionale è robusta (8,1/10), le politiche e norme nazionali sono robuste (7,9/10) e la capacità delle forze dell'ordine è intermedia (7,2/10). Completano il quadro antiriciclaggio 7,4/10, prevenzione 6,5/10 e supporto a vittime e testimoni 5,6/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Taiwan, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati. Poiché l'entità non dispone di una serie nazionale GI-TOC autonoma, i valori derivano da un proxy Celeborn Intelligence ponderato su Giappone 35%, Corea del Sud 35%, Cina 30%; la confidenza deve pertanto essere considerata inferiore e la decisione resa più prudente.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; proxy Celeborn Intelligence ponderato su Giappone 35%, Corea del Sud 35%, Cina 30%. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Taiwan, In Taiwan le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Taiwan, Il livello governativo di Taiwan presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Taiwan, Sul piano militare e dual-use, Taiwan mostra stretta cooperazione con ecosistemi occidentali e capacità dual-use significative. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Taiwan, Personal Data Protection Act, Cyber Security Management Act e disciplina settoriale; elevata capacità tecnologica, ma assenza di decisione UE di adeguatezza. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Taiwan, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 7,2/10 e il rischio sui dati personali è Medio-basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,8	8,1	7,0	8,1	8,3	8,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,1	9,4	7,0	7,7	8,1	7,2

Il GCRI di Taiwan è 8,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 7,9/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Maturità cyber (9,4/10), mentre il più basso è Trasparenza istituzionale (7,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-basso	Medio-basso	Basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 7,9/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Taiwan, la cautela si concentra su 5 ambiti a rischio intermedio: Dati personali, Sanità e biometria, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Taiwan, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Taiwan, Dal punto di vista italiano, Taiwan rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Taiwan è favorevole ma condizionata: il valore FOTR di 7,9/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Trasparenza istituzionale.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.

Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.

Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

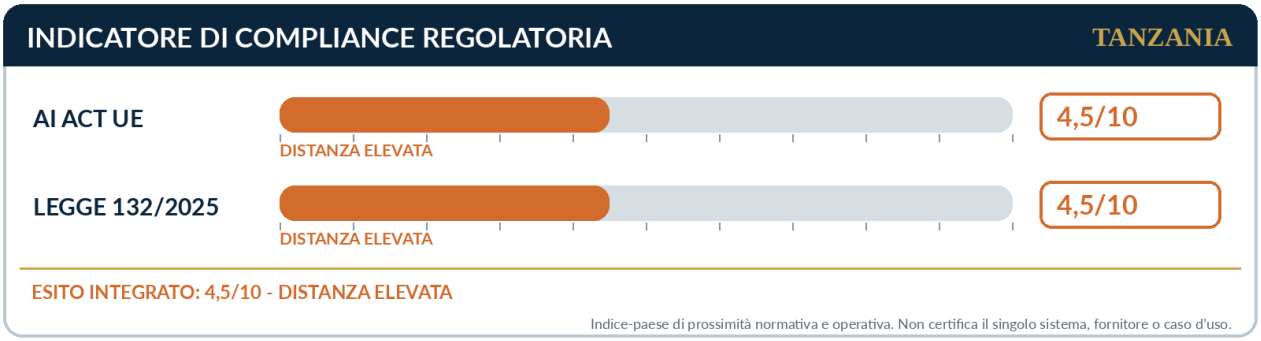
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Taiwan: World Development Indicators, valori più recenti disponibili 2022-2024; World Bank GovTech Maturity Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Bassa con copertura 2/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Tanzania

Posizione FOTR	154	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,5	GCRI / 10	5,1	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Tanzania, AI Act UE 4,5/10; legge 132/2025 4,5/10; esito integrato 4,5/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Tanzania, situato in Africa orientale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 28/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,1/10) e indice FOTR (4,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Tanzania è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	31,2% / 0,2 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	52,4% / 52 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	43,3 / 88,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	99,3/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	41,8/100 - rank 93	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (28/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,0 / 4,2 / 5,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Tanzania, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Tanzania le evidenze principali sono GTMI 88,0/100, EGDI 43,3/100, GCI 99,3/100, AI readiness 41,8/100. La dimensione più robusta è postura di sicurezza cyber (7,9/10), mentre la criticità relativa riguarda maturità infrastrutturale (3,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Tanzania è 3,1/10. La base statistica rileva utenti Internet pari al 31,2% nel 2024; 0,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 52,4% nel 2024; 52 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Tanzania al posto 93 con un valore medio di 41,8/100; il pilastro migliore è adozione pubblica (69,2/100), quello più debole è politiche pubbliche (15,5/100). Il GTMI 2025 è 88,0/100. Il punteggio S2 è 5,1/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Tanzania è valutata fragile, con S3 pari a 4,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 44,0/100, sviluppo e diffusione dell'IA 29,2/100, penetrazione Internet 31,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Tanzania ottiene S4 5,0/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Tanzania, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=5,0/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Tanzania è S5 7,9/10. La base ITU registra ITU GCI 99,3/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è sviluppo delle capacità (19,6/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (28/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,0	Crimini finanziari	6,0
Reti criminali	6,5	Attori incorporati nello Stato	6,0
Attori stranieri	6,0	Attori del settore privato	6,5
Resilienza complessiva	4,2	Cooperazione internazionale	5,0
Politiche e norme nazionali	6,0	Forze dell'ordine	4,0
Antiriciclaggio	4,5	Prevenzione	3,0
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	5,7 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (5,0/10), criminalità finanziaria (6,0/10) e resilienza (4,2/10) colloca Tanzania in una fascia di rischio significativo, pari a 5,7/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (6,5/10) e attori del settore privato (6,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Tanzania assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Tanzania, la resilienza complessiva è debole (4,2/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 3,0/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Tanzania, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Tanzania. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Tanzania, In Tanzania le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner

italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Tanzania, Il livello governativo di Tanzania presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Tanzania, Sul piano militare e dual-use, Tanzania mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Tanzania, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Tanzania, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,0/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,1	5,1	4,4	5,0	7,9	5,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,6	4,4	4,4	5,0	4,2	4,0

Il GCRI di Tanzania è 5,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,0/10), mentre il più basso è Trasferibilità dati (4,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Tanzania, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Tanzania, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Tanzania, Dal punto di vista italiano, Tanzania rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Tanzania ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

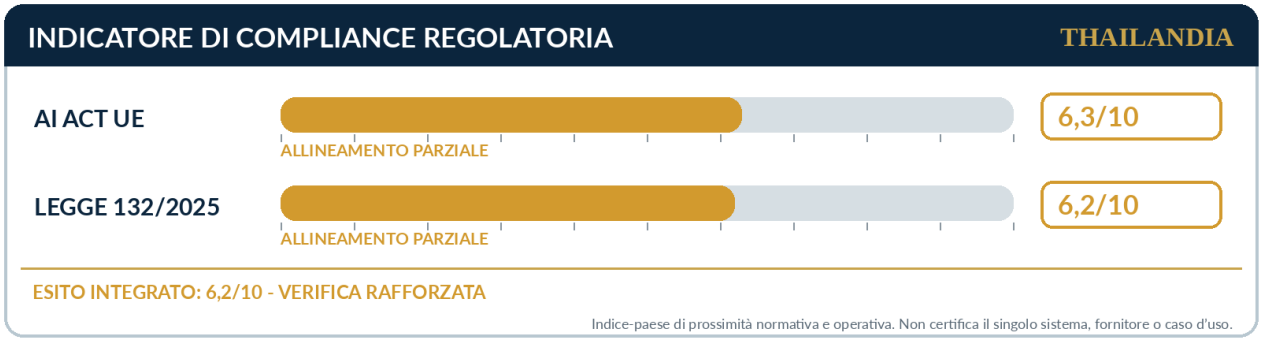
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Tanzania: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Thailandia

Posizione FOTR	69	Area	Asia	Subregione	Asia sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	6,2	GCRI / 10	7,2	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Thailandia, AI Act UE 6,3/10; legge 132/2025 6,2/10; esito integrato 6,2/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Per un operatore italiano, Thailandia non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, Giappone/Corea. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 33/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (7,2/10) è superiore al punteggio FOTR (6,2/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Il quadro di Thailandia è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	90,9% / 14,9 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 3.150 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	83,5 / 83,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	99,2/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	65,1/100 - rank 34	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	39/100 - Non libero / Non libero (33/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,5 / 5,0 / 6,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Thailandia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Thailandia le evidenze principali sono GTMI 83,2/100, EGDI 83,5/100, GCI 99,2/100, AI readiness 65,1/100. La dimensione più robusta è maturità infrastrutturale (8,1/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,4/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Thailandia è 8,1/10. La base statistica rileva utenti Internet pari al 90,9% nel 2024; 14,9 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 3.150 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Thailandia al posto 34 con un valore medio di 65,1/100; il pilastro migliore è politiche pubbliche (88,0/100), quello più debole è resilienza (37,4/100). Il GTMI 2025 è 83,2/100. Il punteggio S2 è 6,9/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Thailandia è valutata sufficiente ma disomogenea, con S3 pari a 6,9/10. Le evidenze disponibili comprendono indice UN di capitale umano 80,3/100, sviluppo e diffusione dell'IA 52,6/100, penetrazione Internet 90,9%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Thailandia ottiene S4 6,4/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, Giappone/Corea; l'indicatore di indipendenza disponibile è 6,2/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Thailandia, Mercato multi-fornitore con gruppi giapponesi, cinesi, statunitensi ed europei. L'impatto sulla valutazione è misurato da S4=6,4/10 e dal proxy di indipendenza 6,2/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Thailandia è S5 7,6/10. La base ITU registra ITU GCI 99,2/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è organizzazione (19,2/20). Freedom on the Net è 39/100 - Non libero, mentre Freedom in the World è Non libero (33/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Personal Data Protection Act 2019, Cybersecurity Act e Computer Crime Act; trasferimenti e accessi pubblici da verificare caso per caso.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,5	Crimini finanziari	8,0
Reti criminali	6,0	Attori incorporati nello Stato	7,0
Attori stranieri	7,5	Attori del settore privato	7,0
Resilienza complessiva	5,0	Cooperazione internazionale	6,5
Politiche e norme nazionali	6,0	Forze dell'ordine	5,5
Antiriciclaggio	5,5	Prevenzione	5,0
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	6,5 - ALTO

Rischio criminale connesso alle tecnologie. In Thailandia il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 6,5/10, livello alto. I reati che dipendono direttamente da sistemi informatici raggiungono 6,5/10; le frodi e i reati finanziari 8,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (7,5/10) e attori incorporati nello Stato (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Thailandia assumono particolare rilevanza centri organizzati di truffa, frodi d'investimento e sentimentali, phishing multicanale, batterie di schede SIM, conti prestanome, riciclaggio in cripto-attività e compromissione di servizi esternalizzati. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Thailandia, la resilienza complessiva è debole (5,0/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è intermedia (5,5/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 5,0/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Thailandia, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; controllo della filiera contro esposizione a complessi organizzati per truffe telematiche, call center coercitivi e conti prestanome; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Thailandia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Thailandia, In Thailandia le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Thailandia, Il livello governativo di Thailandia presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Thailandia, Sul piano militare e dual-use, Thailandia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Thailandia, Personal Data Protection Act 2019, Cybersecurity Act e Computer Crime Act; trasferimenti e accessi pubblici da verificare caso per caso. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Thailandia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 6,1/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,1	6,9	6,9	6,4	7,6	7,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,3	6,7	5,7	6,1	6,2	6,1

Il GCRI di Thailandia è 7,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (6,7/10), mentre il più basso è Trasparenza istituzionale (5,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Thailandia, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Thailandia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Thailandia, Dal punto di vista italiano, Thailandia rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Thailandia è indicata una cooperazione selettiva, coerente con il FOTR di 6,2/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Trasparenza istituzionale a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

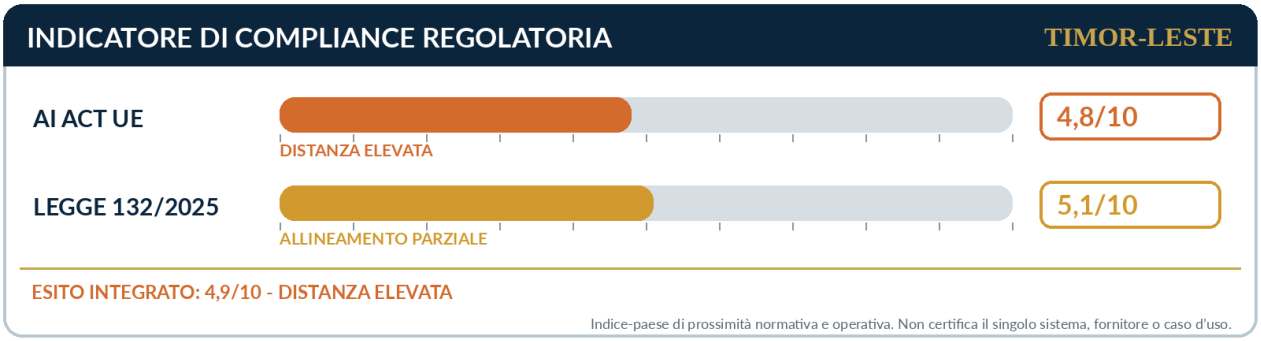
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Thailandia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Timor-Leste

Posizione FOTR	129	Area	Asia	Subregione	Asia sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,2	GCRI / 10	3,5	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Timor-Leste, AI Act UE 4,8/10; legge 132/2025 5,1/10; esito integrato 4,9/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Timor-Leste è stato membro delle nazioni unite collocato in Asia sud-orientale. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 73/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,2/10) supera il GCRI tecnico (3,5/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Per Timor-Leste non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	35,0% / 0,0 per 100	2021/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	94,3% / 265 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	40,2 / 41,0	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	16,8/100 - Tier 5 - capacità iniziali	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	16,8/100 - rank 179	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (73/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Firmatario/invitato	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,5 / 3,9 / 4,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Timor-Leste, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Timor-Leste le evidenze principali sono GTMI 41,0/100, EGDI 40,2/100, GCI 16,8/100, AI readiness 16,8/100. La dimensione più robusta è indipendenza della supply chain (4,3/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,4/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Timor-Leste è 3,8/10. La base statistica rileva utenti Internet pari al 35,0% nel 2021; 0,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 94,3% nel 2024; 265 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Timor-Leste al posto 179 con un valore medio di 16,8/100; il pilastro migliore è infrastrutture IA (24,4/100), quello più debole è governance (3,4/100). Il GTMI 2025 è 41,0/100. Il punteggio S2 è 2,4/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Timor-Leste è valutata fragile, con S3 pari a 3,7/10. Le evidenze disponibili comprendono indice UN di capitale umano 51,0/100, sviluppo e diffusione dell'IA 22,5/100, penetrazione Internet 35,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Timor-Leste ottiene S4 4,3/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Timor-Leste, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo

societario e subfornitura. L'impatto sulla valutazione è misurato da S4=4,3/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Timor-Leste è S5 3,1/10. La base ITU registra ITU GCI 16,8/100, Tier 5 - capacità iniziali; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (73/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Firmatario/invitato. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,5	Crimini finanziari	5,5
Reti criminali	4,0	Attori incorporati nello Stato	4,5
Attori stranieri	5,0	Attori del settore privato	4,0
Resilienza complessiva	3,9	Cooperazione internazionale	4,0
Politiche e norme nazionali	4,0	Forze dell'ordine	4,0
Antiriciclaggio	4,0	Prevenzione	4,5
Supporto vittime e testimoni	3,5	Rischio operativo FOTR-CY	4,5 - MODERATO

Pressione del crimine digitale. Il profilo di Timor-Leste restituisce un rischio FOTR-CY di 4,5/10 (moderato). La componente cyber-dipendente vale 2,5/10 e quella finanziaria 5,5/10; la risposta sistemica è valutata debole, con resilienza media di 3,9/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (5,0/10) e attori incorporati nello Stato (4,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Timor-Leste assumono particolare rilevanza centri organizzati di truffa, frodi d'investimento e sentimentali, phishing multicanale, batterie di schede SIM, conti prestanome, riciclaggio in cripto-attività e compromissione di servizi esternalizzati. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Timor-Leste, la resilienza complessiva è debole (3,9/10); la cooperazione internazionale è debole (4,0/10), le politiche e norme nazionali sono deboli (4,0/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 4,5/10 e supporto a vittime e testimoni 3,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Timor-Leste, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; controllo della filiera contro esposizione a complessi organizzati per truffe telematiche, call center coercitivi e conti prestanome.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Timor-Leste. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Timor-Leste, In Timor-Leste le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Timor-Leste, Il livello governativo di Timor-Leste presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Timor-Leste, Sul piano militare e dual-use, Timor-Leste mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Timor-Leste, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Firmatario/invitato; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Timor-Leste, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,5/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,8	2,4	3,7	4,3	3,1	3,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,0	5,9	4,8	5,3	5,5	4,5

Il GCRI di Timor-Leste è 3,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Maturità cyber (5,9/10), mentre il più basso è Trasferibilità dati (4,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 5,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Timor-Leste, 5 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Timor-Leste, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Timor-Leste, Dal punto di vista italiano, Timor-Leste rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Timor-Leste è indicata una cooperazione selettiva, coerente con il FOTR di 5,2/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

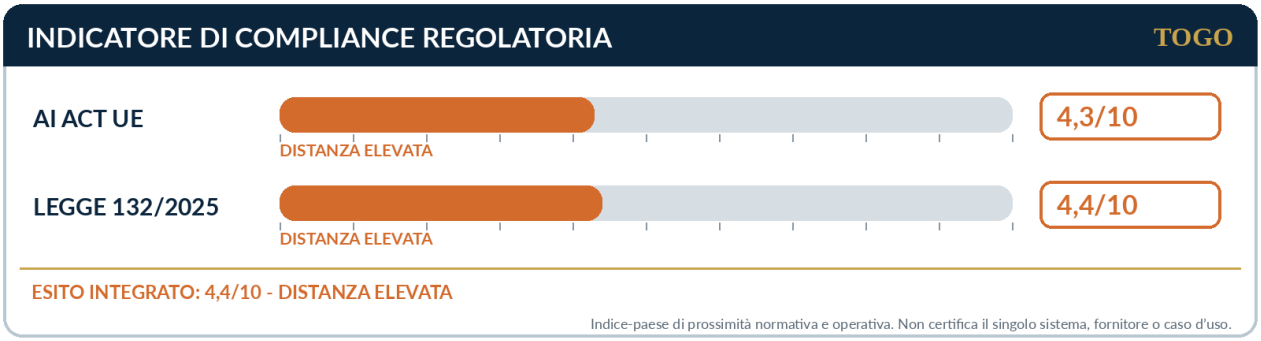
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Timor-Leste: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Togo

Posizione FOTR	169	Area	Africa	Subregione	Africa occidentale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	4,4	GCRI / 10	4,6	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Togo, AI Act UE 4,3/10; legge 132/2025 4,4/10; esito integrato 4,4/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Togo presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 37/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (4,6/10) e indice FOTR (4,4/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Togo è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	39,5% / 1,4 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	61,1% / 102 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	39,2 / 58,7	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	88,8/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	31,9/100 - rank 124	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Parzialmente libero (37/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 4,4 / 5,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Togo, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Togo le evidenze principali sono GTMI 58,7/100, EGDI 39,2/100, GCI 88,8/100, AI readiness 31,9/100. La dimensione più robusta è postura di sicurezza cyber (7,2/10), mentre la criticità relativa riguarda maturità infrastrutturale (3,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Togo è 3,1/10. La base statistica rileva utenti Internet pari al 39,5% nel 2024; 1,4 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 61,1% nel 2024; 102 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Togo al posto 124 con un valore medio di 31,9/100; il pilastro migliore è governance (55,0/100), quello più debole è sviluppo e diffusione (12,0/100). Il GTMI 2025 è 58,7/100. Il punteggio S2 è 3,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Togo è valutata fragile, con S3 pari a 4,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 48,1/100, sviluppo e diffusione dell'IA 12,0/100, penetrazione Internet 39,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Togo ottiene S4 4,9/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Togo, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,9/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Togo è S5 7,2/10. La base ITU registra ITU GCI 88,8/100, Tier 2 - avanzato; il pilastro relativamente più debole è misure tecniche (15,3/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Parzialmente libero (37/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	4,0
Reti criminali	7,0	Attori incorporati nello Stato	7,5
Attori stranieri	7,5	Attori del settore privato	6,0
Resilienza complessiva	4,4	Cooperazione internazionale	6,0
Politiche e norme nazionali	5,5	Forze dell'ordine	5,0
Antiriciclaggio	3,5	Prevenzione	5,0
Supporto vittime e testimoni	5,0	Rischio operativo FOTR-CY	5,1 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (3,0/10), criminalità finanziaria (4,0/10) e resilienza (4,4/10) colloca Togo in una fascia di rischio significativo, pari a 5,1/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,5/10) e attori stranieri (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Togo assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Togo, la resilienza complessiva è debole (4,4/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 5,0/10 e supporto a vittime e testimoni 5,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Togo, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Togo. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Togo, In Togo le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Togo, Il livello governativo di Togo presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Togo, Sul piano militare e dual-use, Togo mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Togo, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Togo, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,3/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,1	3,9	4,0	4,9	7,2	4,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,4	4,3	4,2	5,0	4,4	4,3

Il GCRI di Togo è 4,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,0/10), mentre il più basso è Trasparenza istituzionale (4,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Togo, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Togo, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Togo, Dal punto di vista italiano, Togo rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Togo ricade nella fascia di alto rischio (4,4/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.
Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

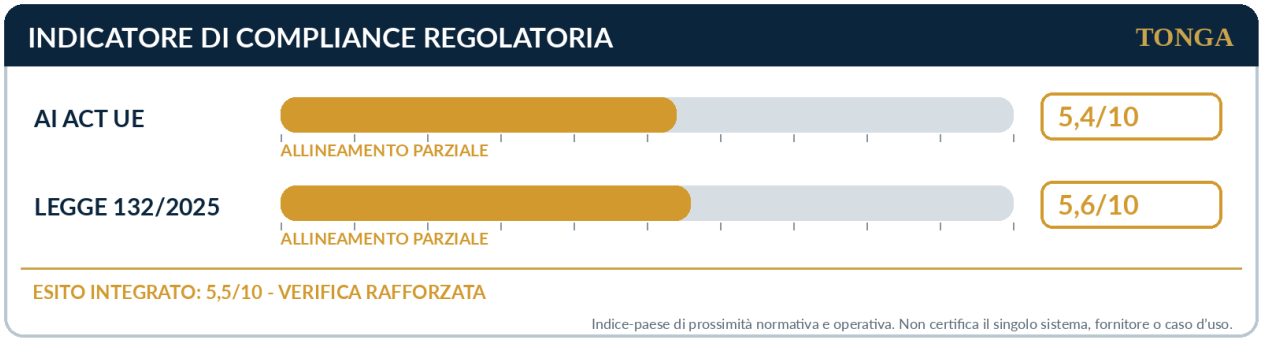
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Togo: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Tonga

Posizione FOTR	105	Area	Oceania	Subregione	Pacifico insulare
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,7	GCRI / 10	4,2	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Tonga, AI Act UE 5,4/10; legge 132/2025 5,6/10; esito integrato 5,5/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Tonga, situato in Pacifico insulare, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La distanza geografica e l'insularità rendono centrali cavi sottomarini, satelliti, continuità energetica e dipendenza da fornitori australiani, neozelandesi, statunitensi o asiatici. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 79/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,7/10) supera il GCRI tecnico (4,2/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Tonga dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	67,4% / 8,2 per 100	2024/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 970 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	51,6 / 34,3	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	33,8/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	21,4/100 - rank 156	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (79/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,5 / 5,2 / 4,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Tonga, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Tonga le evidenze principali sono GTMI 34,3/100, EGDI 51,6/100, GCI 33,8/100, AI readiness 21,4/100. La dimensione più robusta è maturità infrastrutturale (5,5/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,6/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Tonga è 5,5/10. La base statistica rileva utenti Internet pari al 67,4% nel 2024; 8,2 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 100,0% nel 2024; 970 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Tonga al posto 156 con un valore medio di 21,4/100; il pilastro migliore è resilienza (32,7/100), quello più debole è politiche pubbliche (4,0/100). Il GTMI 2025 è 34,3/100. Il punteggio S2 è 2,6/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Tonga è valutata sufficiente ma disomogenea, con S3 pari a 5,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 74,9/100, sviluppo e diffusione dell'IA 24,1/100, penetrazione Internet 67,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Tonga ottiene S4 4,0/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Tonga, Dipendenza da Australia, Nuova Zelanda, Stati Uniti, Francia e operatori satellitari o sottomarini; la scala ridotta limita la diversificazione e aumenta il rischio di concentrazione. L'impatto sulla

valutazione è misurato da S4=4,0/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Tonga è S5 4,1/10. La base ITU registra ITU GCI 33,8/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è sviluppo delle capacità (2,9/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (79/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,5	Crimini finanziari	4,0
Reti criminali	4,5	Attori incorporati nello Stato	6,0
Attori stranieri	6,0	Attori del settore privato	1,5
Resilienza complessiva	5,2	Cooperazione internazionale	6,5
Politiche e norme nazionali	6,5	Forze dell'ordine	6,0
Antiriciclaggio	5,0	Prevenzione	4,0
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	4,2 - MODERATO

Rischio criminale connesso alle tecnologie. In Tonga il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 4,2/10, livello moderato. I reati che dipendono direttamente da sistemi informatici raggiungono 2,5/10; le frodi e i reati finanziari 4,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (6,0/10) e attori stranieri (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Tonga assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Tonga, la resilienza complessiva è debole (5,2/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è intermedia (6,0/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Tonga, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Tonga. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Tonga, In Tonga le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Tonga, Il livello governativo di Tonga presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Tonga, Sul piano militare e dual-use, Tonga mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Tonga, Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Tonga, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,4/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
5,5	2,6	5,0	4,0	4,1	4,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,8	5,2	5,9	6,6	4,8	5,4

Il GCRI di Tonga è 4,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,6/10), mentre il più basso è Supply chain (4,8/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio-alto	Medio	Medio	Medio

La matrice applica il FOTR di 5,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Tonga, 1 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Cloud e infrastrutture. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Tonga, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Tonga, Dal punto di vista italiano, Tonga rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Tonga è indicata una cooperazione selettiva, coerente con il FOTR di 5,7/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Cloud e infrastrutture a decisione caso per caso.

Presidi minimi raccomandati

- Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
- Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
- Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
- Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

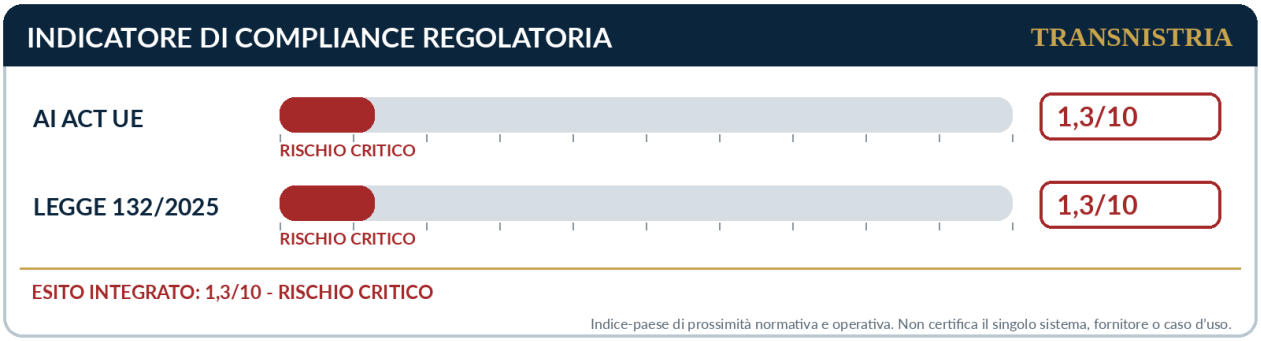
Profilo Celeborn Intelligence di Tonga: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom

House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Transnistria

Posizione FOTR	201	Area	Europa	Subregione	Europa orientale
Status	Entità de facto non riconosciuta	Confidenza Celeborn Intelligence	Bassa	Copertura dati	0/7 famiglie
FOTR / 10	1,2	GCRI / 10	1,6	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Transnistria, AI Act UE 1,3/10; legge 132/2025 1,3/10; esito integrato 1,3/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Per un operatore italiano, Transnistria non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La prossimità europea può ridurre i costi operativi, ma non sostituisce la verifica dell'allineamento al GDPR, delle autorità indipendenti e della reale origine dei servizi cloud. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Russia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 16/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (1,6/10) e indice FOTR (1,2/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Entità de facto non riconosciuta, integrata economicamente e tecnologicamente con reti regionali ma esposta a dipendenze russe e incertezza giuridica.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	n.d. / n.d. per 100	n.d./n.d.	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	n.d. / n.d. per milione	n.d./n.d.	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	n.d. / n.d.	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	n.d./100 - n.d.	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	n.d./100 - rank n.d.	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (16/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	8,3 / 3,7 / 7,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Transnistria, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 0/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Transnistria le evidenze principali sono nessun indicatore composito pienamente comparabile. La dimensione più robusta è indipendenza della supply chain (3,0/10), mentre la criticità relativa riguarda capitale umano e competenze digitali (0,1/10). Sono disponibili 0 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata bassa. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Transnistria è 1,9/10. La base statistica rileva i principali dati WDI non sono disponibili in forma omogenea. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Per Transnistria non è disponibile un profilo Oxford Insights direttamente attribuibile; l'adozione di IA è quindi valutata attraverso GovTech, servizi online, infrastrutture e fonti qualitative. Il punteggio S2 è 1,6/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Transnistria è valutata fragile, con S3 pari a 0,1/10. Le evidenze disponibili comprendono evidenza quantitativa incompleta. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Transnistria ottiene S4 3,0/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Russia; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Transnistria, Dipendenza da infrastrutture moldove e regionali, con forte influenza russa e catene poco trasparenti. L'impatto sulla valutazione è misurato da S4=3,0/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Transnistria è S5 1,5/10. La base ITU registra GCI non disponibile in forma comparabile. Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (16/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Disciplina nazionale della protezione dei dati, delle comunicazioni elettroniche e dei reati informatici, con differenze rispetto al GDPR; trasferimenti e accessi pubblici richiedono una verifica locale aggiornata.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	8,3	Crimini finanziari	8,3
Reti criminali	6,1	Attori incorporati nello Stato	8,6
Attori stranieri	5,2	Attori del settore privato	7,6
Resilienza complessiva	3,7	Cooperazione internazionale	4,1
Politiche e norme nazionali	5,5	Forze dell'ordine	4,0
Antiriciclaggio	3,7	Prevenzione	3,2
Supporto vittime e testimoni	3,2	Rischio operativo FOTR-CY	7,6 - ALTO

Rischio criminale connesso alle tecnologie. In Transnistria il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 7,6/10, livello alto. I reati che dipendono direttamente da sistemi informatici raggiungono 8,3/10; le frodi e i reati finanziari 8,3/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,6/10) e attori del settore privato (7,6/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Transnistria assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Transnistria, la resilienza complessiva è debole (3,7/10); la cooperazione internazionale è debole (4,1/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 3,7/10, prevenzione 3,2/10 e supporto a vittime e testimoni 3,2/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Transnistria, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; blocco di hosting e ASN ad alta reputazione negativa, ricerca proattiva delle minacce su malware sottrattori di informazioni e controllo dei canali RDP/VPN; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE. Poiché l'entità non dispone di una serie nazionale GI-TOC autonoma, i valori derivano da un proxy Celeborn Intelligence ponderato su Moldova 45%, Federazione Russa 55%; la confidenza deve pertanto essere considerata inferiore e la decisione resa più prudente.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; proxy Celeborn Intelligence ponderato su Moldova 45%, Federazione Russa 55%. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Transnistria, In Transnistria le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture

esterne. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Transnistria, Il livello governativo di Transnistria presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Transnistria, Sul piano militare e dual-use, Transnistria mostra forte integrazione o dipendenza dall'ecosistema russo, inclusi sistemi di comando, comunicazione e sicurezza. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Transnistria, Disciplina nazionale della protezione dei dati, delle comunicazioni elettroniche e dei reati informatici, con differenze rispetto al GDPR; trasferimenti e accessi pubblici richiedono una verifica locale aggiornata. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Transnistria, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 0,0/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
1,9	1,6	0,1	3,0	1,5	1,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
2,4	2,3	0,1	0,4	1,8	0,0

Il GCRI di Transnistria è 1,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 1,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (2,4/10), mentre il più basso è Trasferibilità dati (0,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 1,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Transnistria, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Transnistria, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Transnistria, Dal punto di vista italiano, Transnistria rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Transnistria, il FOTR di 1,2/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

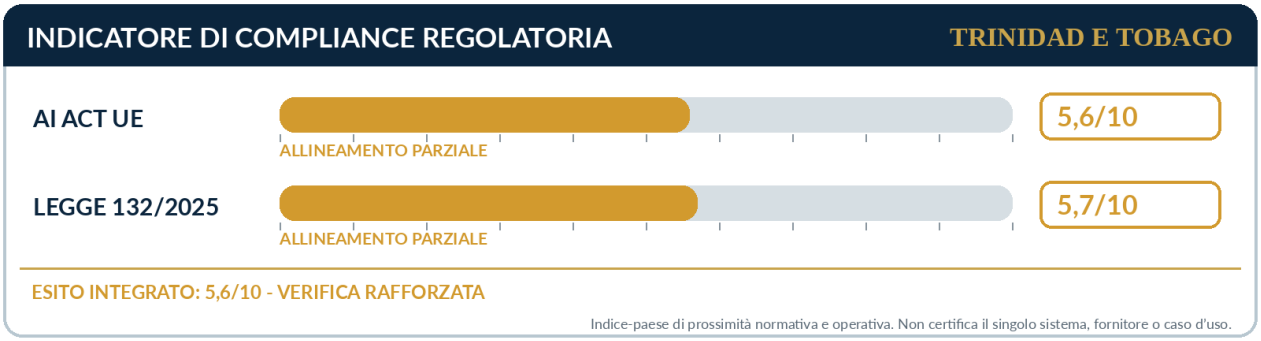
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Transnistria: World Development Indicators, valori più recenti disponibili 2022-2024; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Bassa con copertura 0/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Trinidad e Tobago

Posizione FOTR	106	Area	Americhe	Subregione	Caraibi
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,7	GCRI / 10	5,4	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Trinidad e Tobago, AI Act UE 5,6/10; legge 132/2025 5,7/10; esito integrato 5,6/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Trinidad e Tobago è stato membro delle nazioni unite collocato in Caraibi. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 83/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,4/10) e indice FOTR (5,7/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. In Trinidad e Tobago la trasformazione digitale procede più rapidamente dell'uniformità regolatoria e operativa. Gli investimenti devono essere accompagnati da audit, clausole di uscita e gestione locale del rischio.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	82,2% / 27,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 480 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	69,7 / 45,9	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	56,2/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	32,9/100 - rank 120	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (83/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Firmatario/invitato	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,5 / 5,1 / 5,9	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Trinidad e Tobago, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Trinidad e Tobago le evidenze principali sono GTMI 45,9/100, EGDI 69,7/100, GCI 56,2/100, AI readiness 32,9/100. La dimensione più robusta è maturità infrastrutturale (7,7/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (4,0/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Trinidad e Tobago è 7,7/10. La base statistica rileva utenti Internet pari al 82,2% nel 2024; 27,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 480 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Trinidad e Tobago al posto 120 con un valore medio di 32,9/100; il pilastro migliore è infrastrutture IA (46,6/100), quello più debole è sviluppo e diffusione (12,7/100). Il GTMI 2025 è 45,9/100. Il punteggio S2 è 4,0/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Trinidad e Tobago è valutata sufficiente ma disomogenea, con S3 pari a 5,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 71,7/100, sviluppo e diffusione dell'IA 12,7/100, penetrazione Internet 82,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Trinidad e Tobago ottiene S4 4,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Trinidad e Tobago, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto

sulla valutazione è misurato da S4=4,6/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Trinidad e Tobago è S5 5,6/10. La base ITU registra ITU GCI 56,2/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è misure tecniche (7,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (83/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Firmatario/invitato. Quadro normativo sintetico: Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,5	Crimini finanziari	6,5
Reti criminali	6,0	Attori incorporati nello Stato	5,0
Attori stranieri	6,5	Attori del settore privato	4,0
Resilienza complessiva	5,1	Cooperazione internazionale	6,5
Politiche e norme nazionali	7,0	Forze dell'ordine	4,0
Antiriciclaggio	5,0	Prevenzione	5,0
Supporto vittime e testimoni	5,5	Rischio operativo FOTR-CY	5,9 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Trinidad e Tobago presenta un'esposizione stimata significativa (5,9/10): reati cyber-dipendenti 6,5/10, crimini finanziari 6,5/10 e resilienza 5,1/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (6,5/10) e reti criminali (6,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Trinidad e Tobago assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Trinidad e Tobago, la resilienza complessiva è debole (5,1/10); la cooperazione internazionale è intermedia (6,5/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 5,0/10 e supporto a vittime e testimoni 5,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Trinidad e Tobago, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Trinidad e Tobago. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Trinidad e Tobago, In Trinidad e Tobago le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La

superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Trinidad e Tobago, Il livello governativo di Trinidad e Tobago presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Trinidad e Tobago, Sul piano militare e dual-use, Trinidad e Tobago mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Trinidad e Tobago, Normativa nazionale o settoriale su privacy, telecomunicazioni e reati informatici, con livello di vigilanza variabile. In assenza di adeguatezza UE sono necessari strumenti del capo V GDPR e verifica dei rimedi effettivi. Lo stato rispetto alla Convenzione di Budapest è: Firmatario/invitato; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Trinidad e Tobago, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,4/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,7	4,0	5,1	4,6	5,6	5,4

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,0	5,2	5,9	6,2	5,4	5,4

Il GCRI di Trinidad e Tobago è 5,4/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,2/10), mentre il più basso è Maturità cyber (5,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 5,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Trinidad e Tobago, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Trinidad e Tobago, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Trinidad e Tobago, Dal punto di vista italiano, Trinidad e Tobago rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Trinidad e Tobago è indicata una cooperazione selettiva, coerente con il FOTR di 5,7/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Maturità cyber a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.

Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

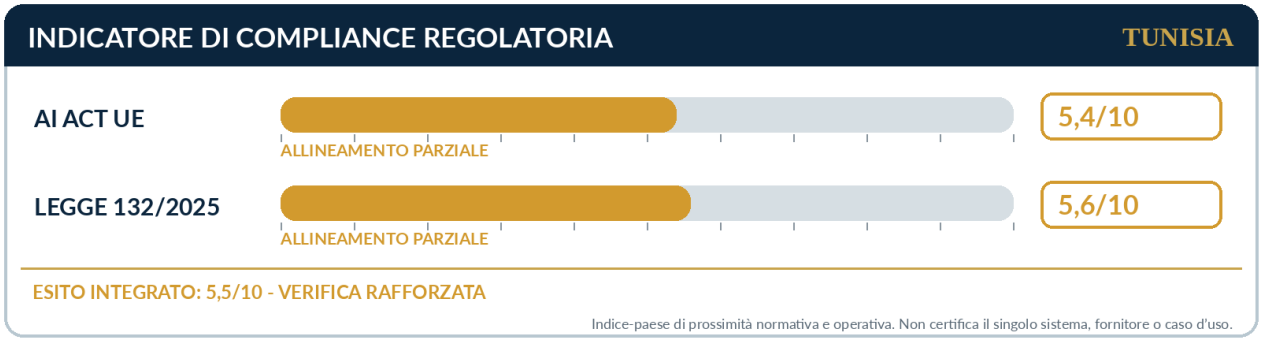
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Trinidad e Tobago: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Tunisia

Posizione FOTR	118	Area	Africa	Subregione	Africa settentrionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,5	GCRI / 10	6,0	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Tunisia, AI Act UE 5,4/10; legge 132/2025 5,6/10; esito integrato 5,5/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Nel quadro di Africa, Tunisia presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 42/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,0/10) e indice FOTR (5,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Tunisia dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	76,5% / 15,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 912 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	69,3 / 71,5	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	82,0/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	41,1/100 - rank 88	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	59/100 - Parzialmente libero / Parzialmente libero (42/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,0 / 4,3 / 5,3	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Tunisia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Tunisia le evidenze principali sono GTMI 71,5/100, EGDI 69,3/100, GCI 82,0/100, AI readiness 41,1/100. La dimensione più robusta è maturità infrastrutturale (7,3/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (5,0/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Tunisia è 7,3/10. La base statistica rileva utenti Internet pari al 76,5% nel 2024; 15,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 912 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Tunisia al posto 88 con un valore medio di 41,1/100; il pilastro migliore è governance (59,0/100), quello più debole è politiche pubbliche (19,5/100). Il GTMI 2025 è 71,5/100. Il punteggio S2 è 5,0/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Tunisia è valutata sufficiente ma disomogenea, con S3 pari a 5,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 65,0/100, sviluppo e diffusione dell'IA 36,7/100, penetrazione Internet 76,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Tunisia ottiene S4 5,4/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Tunisia, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=5,4/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Tunisia è S5 6,9/10. La base ITU registra ITU GCI 82,0/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è organizzazione (14,2/20). Freedom on the Net è 59/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (42/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge organica 2004-63 e quadro cyber nazionale; riforma della protezione dati necessaria per piena convergenza europea.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,0	Crimini finanziari	8,0
Reti criminali	4,5	Attori incorporati nello Stato	6,5
Attori stranieri	4,0	Attori del settore privato	4,5
Resilienza complessiva	4,3	Cooperazione internazionale	5,5
Politiche e norme nazionali	6,0	Forze dell'ordine	5,0
Antiriciclaggio	5,5	Prevenzione	3,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	5,3 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Tunisia restituisce un rischio FOTR-CY di 5,3/10 (significativo). La componente cyber-dipendente vale 4,0/10 e quella finanziaria 8,0/10; la risposta sistemica è valutata debole, con resilienza media di 4,3/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (6,5/10) e reti criminali (4,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Tunisia assumono particolare rilevanza phishing e credential theft, ransomware, frodi d'investimento, attacchi a energia e servizi pubblici, abuso di cripto-attività e campagne che possono combinare profitto, spionaggio e pressione politica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Tunisia, la resilienza complessiva è debole (4,3/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 3,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Tunisia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Tunisia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Tunisia, In Tunisia le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Tunisia, Il livello governativo di Tunisia presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Tunisia, Sul piano militare e dual-use, Tunisia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Tunisia, Legge organica 2004-63 e quadro cyber nazionale; riforma della protezione dati necessaria per piena convergenza europea. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Tunisia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,1/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,3	5,0	5,5	5,4	6,9	6,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,7	5,3	5,3	6,2	5,4	5,1

Il GCRI di Tunisia è 6,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,2/10), mentre il più basso è Trasferibilità dati (5,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio	Medio-alto	Medio-alto	Medio

La matrice applica il FOTR di 5,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Tunisia, 4 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, IP e R&S, Pubblica amministrazione. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Tunisia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Tunisia, Dal punto di vista italiano, Tunisia rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Tunisia è indicata una cooperazione selettiva, coerente con il FOTR di 5,5/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

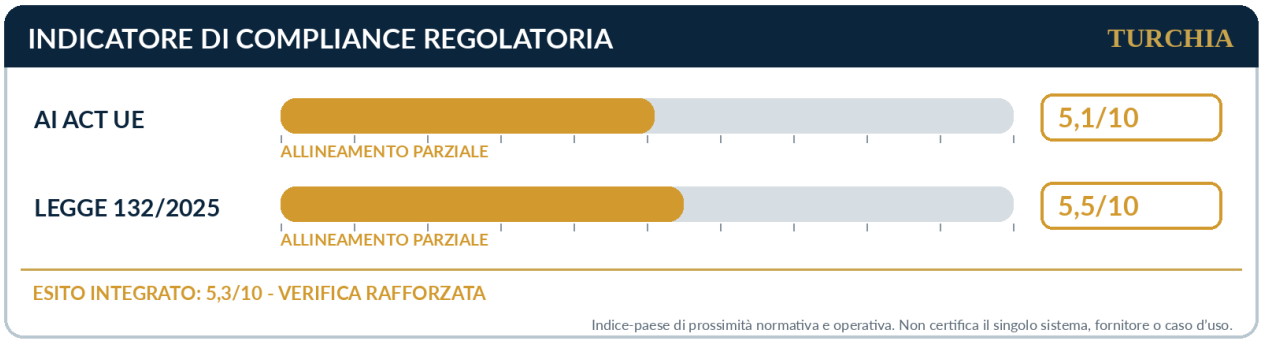
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Tunisia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Turchia

Posizione FOTR	130	Area	Asia	Subregione	Anatolia e Mediterraneo orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	5,2	GCRI / 10	6,9	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Turchia, AI Act UE 5,1/10; legge 132/2025 5,5/10; esito integrato 5,3/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Turchia, situato in Anatolia e Mediterraneo orientale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La collocazione nell'Alleanza Atlantica favorisce interoperabilità e cooperazione di sicurezza, senza equivalere automaticamente ad allineamento pieno sul diritto dei dati. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 32/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (6,9/10) è superiore al punteggio FOTR (5,2/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Turchia presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	89,8% / 23,4 per 100	2025/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 11.103 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	89,1 / 81,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	100,0/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	61,4/100 - rank 53	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	31/100 - Non libero / Non libero (32/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 4,0 / 6,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Turchia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Turchia le evidenze principali sono GTMI 81,2/100, EGDI 89,1/100, GCI 100,0/100, AI readiness 61,4/100. La dimensione più robusta è maturità infrastrutturale (8,2/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,3/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Turchia è 8,2/10. La base statistica rileva utenti Internet pari al 89,8% nel 2025; 23,4 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 11.103 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Turchia al posto 53 con un valore medio di 61,4/100; il pilastro migliore è adozione pubblica (77,6/100), quello più debole è sviluppo e diffusione (45,7/100). Il GTMI 2025 è 81,2/100. Il punteggio S2 è 6,8/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Turchia è valutata sufficiente ma disomogenea, con S3 pari a 7,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 91,9/100, sviluppo e diffusione dell'IA 45,7/100, penetrazione Internet 89,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Turchia ottiene S4 5,3/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Turchia, Forte base domestica, soprattutto nel dual-use, integrata con fornitori europei, statunitensi e asiatici. L'impatto sulla valutazione è misurato da S4=5,3/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Turchia è S5 7,2/10. La base ITU registra ITU GCI 100,0/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è misure giuridiche (20,0/20). Freedom on the Net è 31/100 - Non libero, mentre Freedom in the World è Non libero (32/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge 6698 sulla protezione dei dati, disciplina BTK e normativa cyber; trasferimenti e localizzazione richiedono verifica normativa e autorizzativa.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	8,5
Reti criminali	8,0	Attori incorporati nello Stato	9,0
Attori stranieri	6,5	Attori del settore privato	6,0
Resilienza complessiva	4,0	Cooperazione internazionale	5,0
Politiche e norme nazionali	5,0	Forze dell'ordine	3,5
Antiriciclaggio	3,0	Prevenzione	3,5
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	6,8 - ALTO

Quadro criminale digitale. Per Turchia, l'indice operativo FOTR-CY è 6,8/10, classe alta. Il mercato dei reati cyber-dipendenti è elevato (5,5/10), mentre i crimini finanziari sono molto elevati (8,5/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e reti criminali (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Turchia assumono particolare rilevanza ransomware, phishing, furto di credenziali, frodi finanziarie, compromissione di terze parti, estorsione dei dati e riciclaggio digitale transfrontaliero. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Turchia, la resilienza complessiva è debole (4,0/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è debole (3,5/10). Completano il quadro antiriciclaggio 3,0/10, prevenzione 3,5/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Turchia, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Turchia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Turchia, In Turchia le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner

italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Turchia, Il livello governativo di Turchia presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Turchia, Sul piano militare e dual-use, Turchia mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Turchia, Legge 6698 sulla protezione dei dati, disciplina BTK e normativa cyber; trasferimenti e localizzazione richiedono verifica normativa e autorizzativa. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Turchia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 3,2/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,2	6,8	7,0	5,3	7,2	6,9

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,0	6,0	4,4	7,4	4,8	3,2

Il GCRI di Turchia è 6,9/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,2/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (7,4/10), mentre il più basso è Trasferibilità dati (3,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio	Medio-alto	Medio	Medio

La matrice applica il FOTR di 5,2/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Turchia, 3 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, IP e R&S. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Turchia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Turchia, Dal punto di vista italiano, Turchia rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Turchia è indicata una cooperazione selettiva, coerente con il FOTR di 5,2/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Dati personali a decisione caso per caso.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.
Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

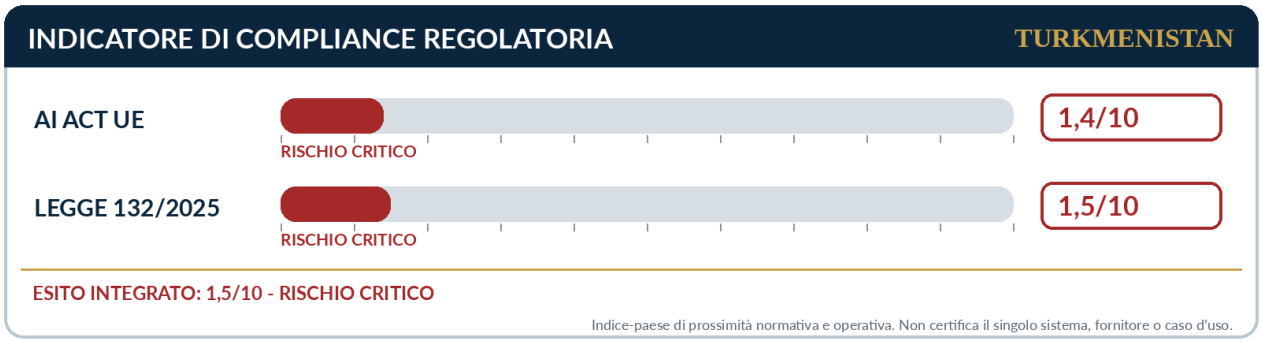
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Turchia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Turkmenistan

Posizione FOTR	197	Area	Asia	Subregione	Caucaso e Asia centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	1,4	GCRI / 10	3,3	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Turkmenistan, AI Act UE 1,4/10; legge 132/2025 1,5/10; esito integrato 1,5/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Per un operatore italiano, Turkmenistan non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina, Russia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 1/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (3,3/10) è superiore al punteggio FOTR (1,4/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Per Turkmenistan la regola operativa è evitare trasferimenti e dipendenze tecnologiche, salvo finalità umanitarie o istituzionali autorizzate e protette da architetture isolate. Il contratto, da solo, non rende il rischio accettabile.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	18,0% / 5,2 per 100	2016/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 188 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	47,6 / 14,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	25,9/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	21,1/100 - rank 159	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (1/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,5 / 2,2 / 5,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Turkmenistan, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Turkmenistan le evidenze principali sono GTMI 14,6/100, EGDI 47,6/100, GCI 25,9/100, AI readiness 21,1/100. La dimensione più robusta è maturità infrastrutturale (4,2/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (2,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Turkmenistan è 4,2/10. La base statistica rileva utenti Internet pari al 18,0% nel 2016; 5,2 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 100,0% nel 2024; 188 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Turkmenistan al posto 159 con un valore medio di 21,1/100; il pilastro migliore è infrastrutture IA (32,6/100), quello più debole è adozione pubblica (8,1/100). Il GTMI 2025 è 14,6/100. Il punteggio S2 è 2,1/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Turkmenistan è valutata fragile, con S3 pari a 3,9/10. Le evidenze disponibili comprendono indice UN di capitale umano 66,1/100, sviluppo e diffusione dell'IA 22,5/100, penetrazione Internet 18,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Turkmenistan ottiene S4 3,7/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina, Russia; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Turkmenistan, Prevalenza di forniture cinesi e russe in un mercato fortemente controllato dallo Stato. L'impatto sulla valutazione è misurato da S4=3,7/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Turkmenistan è S5 2,4/10. La base ITU registra ITU GCI 25,9/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (1/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa formale sui dati accompagnata da controllo statale esteso e connettività fortemente limitata; trasferimenti strategici sconsigliati.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,5	Crimini finanziari	6,5
Reti criminali	4,5	Attori incorporati nello Stato	9,0
Attori stranieri	3,5	Attori del settore privato	2,5
Resilienza complessiva	2,2	Cooperazione internazionale	1,5
Politiche e norme nazionali	2,5	Forze dell'ordine	2,0
Antiriciclaggio	3,0	Prevenzione	2,0
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	5,6 - SIGNIFICATIVO

Pressione del crimine digitale. Il profilo di Turkmenistan restituisce un rischio FOTR-CY di 5,6/10 (significativo). La componente cyber-dipendente vale 2,5/10 e quella finanziaria 6,5/10; la risposta sistemica è valutata molto debole, con resilienza media di 2,2/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e reti criminali (4,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Turkmenistan assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Turkmenistan, la resilienza complessiva è molto debole (2,2/10); la cooperazione internazionale è molto debole (1,5/10), le politiche e norme nazionali sono molto deboli (2,5/10) e la capacità delle forze dell'ordine è molto debole (2,0/10). Completano il quadro antiriciclaggio 3,0/10, prevenzione 2,0/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Turkmenistan, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; blocco di hosting e ASN ad alta reputazione negativa, ricerca proattiva delle minacce su malware sottrattori di informazioni e controllo dei canali RDP/VPN; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Turkmenistan. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Turkmenistan, In Turkmenistan le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture

esterne. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Turkmenistan, Il livello governativo di Turkmenistan presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Turkmenistan, Sul piano militare e dual-use, Turkmenistan mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Turkmenistan, Normativa formale sui dati accompagnata da controllo statale esteso e connettività fortemente limitata; trasferimenti strategici sconsigliati. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Turkmenistan, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 0,4/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
4,2	2,1	3,9	3,7	2,4	3,3

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
1,5	3,1	0,0	1,3	2,4	0,4

Il GCRI di Turkmenistan è 3,3/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 1,4/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (3,1/10), mentre il più basso è Trasparenza istituzionale (0,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Estremo	Estremo	Estremo	Estremo

La matrice applica il FOTR di 1,4/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Turkmenistan, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Turkmenistan, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Turkmenistan, Dal punto di vista italiano, Turkmenistan rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Turkmenistan, il FOTR di 1,4/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.

Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.

Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.

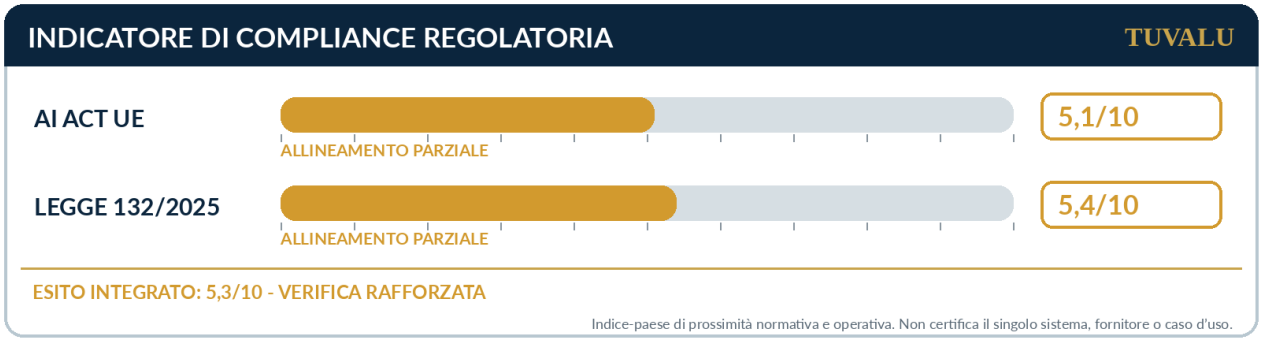
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Turkmenistan: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Tuvalu

Posizione FOTR	119	Area	Oceania	Subregione	Pacifico insulare
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,5	GCRI / 10	3,5	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Tuvalu, AI Act UE 5,1/10; legge 132/2025 5,4/10; esito integrato 5,3/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Tuvalu è stato membro delle nazioni unite collocato in Pacifico insulare. La distanza geografica e l'insularità rendono centrali cavi sottomarini, satelliti, continuità energetica e dipendenza da fornitori australiani, neozelandesi, statunitensi o asiatici. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 93/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,5/10) supera il GCRI tecnico (3,5/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Il quadro di Tuvalu è adatto a iniziative mirate, purché il progetto separi le funzioni ordinarie da quelle sensibili e preveda controlli su sicurezza, subfornitura e continuità.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	35,2% / 4,5 per 100	2017/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 311 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	40,4 / 12,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	20,3/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	17,7/100 - rank 169	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (93/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	1,0 / 5,9 / 2,1	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Tuvalu, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Tuvalu le evidenze principali sono GTMI 12,4/100, EGDI 40,4/100, GCI 20,3/100, AI readiness 17,7/100. La dimensione più robusta è maturità infrastrutturale (4,5/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (1,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Tuvalu è 4,5/10. La base statistica rileva utenti Internet pari al 35,2% nel 2017; 4,5 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 100,0% nel 2024; 311 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Tuvalu al posto 169 con un valore medio di 17,7/100; il pilastro migliore è infrastrutture IA (39,5/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 12,4/100. Il punteggio S2 è 1,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Tuvalu è valutata fragile, con S3 pari a 4,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 54,6/100, sviluppo e diffusione dell'IA 25,0/100, penetrazione Internet 35,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Tuvalu ottiene S4 4,0/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Tuvalu, Dipendenza da Australia, Nuova Zelanda, Stati Uniti, Francia e operatori satellitari o sottomarini; la scala ridotta limita la diversificazione e aumenta il rischio di concentrazione. L'impatto sulla

valutazione è misurato da S4=4,0/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Tuvalu è S5 3,1/10. La base ITU registra ITU GCI 20,3/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (93/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	1,0	Crimini finanziari	2,0
Reti criminali	1,0	Attori incorporati nello Stato	1,5
Attori stranieri	2,5	Attori del settore privato	1,0
Resilienza complessiva	5,9	Cooperazione internazionale	5,5
Politiche e norme nazionali	6,5	Forze dell'ordine	7,0
Antiriciclaggio	6,0	Prevenzione	4,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	2,1 - CONTENUTO

Pressione del crimine digitale. Il profilo di Tuvalu restituisce un rischio FOTR-CY di 2,1/10 (contenuto). La componente cyber-dipendente vale 1,0/10 e quella finanziaria 2,0/10; la risposta sistemica è valutata intermedia, con resilienza media di 5,9/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (2,5/10) e attori incorporati nello Stato (1,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Tuvalu assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Tuvalu, la resilienza complessiva è intermedia (5,9/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è intermedia (7,0/10). Completano il quadro antiriciclaggio 6,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Tuvalu, il livello contenuto non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Tuvalu. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Tuvalu, In Tuvalu le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Tuvalu, Il livello governativo di Tuvalu presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. L'affidabilità deve

essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Tuvalu, Sul piano militare e dual-use, Tuvalu mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Tuvalu, Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Tuvalu, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,0/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
4,5	1,9	4,0	4,0	3,1	3,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
6,0	4,7	5,7	6,4	4,7	5,0

Il GCRI di Tuvalu è 3,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,4/10), mentre il più basso è Maturità cyber (4,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio-alto	Medio	Medio-alto	Medio

La matrice applica il FOTR di 5,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Tuvalu, 2 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Cloud e infrastrutture, Pubblica amministrazione. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Tuvalu, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Tuvalu, Dal punto di vista italiano, Tuvalu rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Tuvalu è indicata una cooperazione selettiva, coerente con il FOTR di 5,5/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Cloud e infrastrutture a decisione caso per caso.

Presidi minimi raccomandati

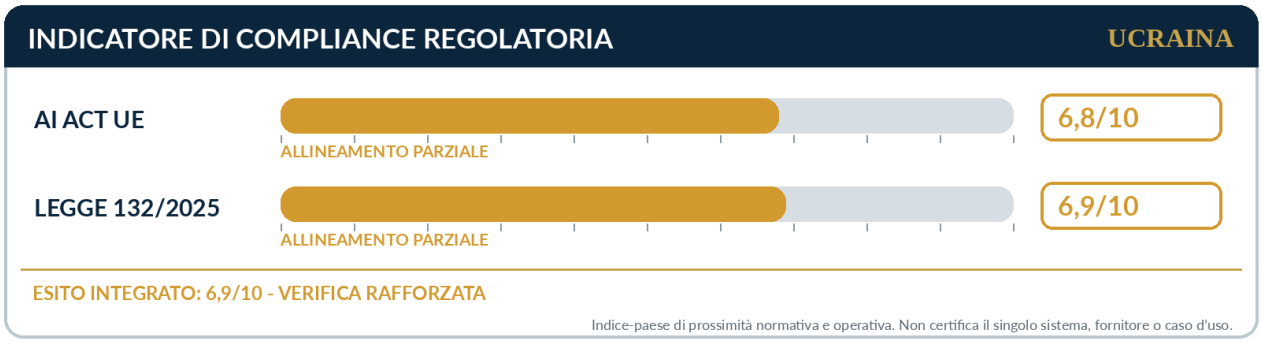
Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Tuvalu: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Ucraina

Posizione FOTR	55	Area	Europa	Subregione	Europa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	6,7	GCRI / 10	6,6	Classe operativa	Affidabilità favorevole ma condizionata

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Ucraina, AI Act UE 6,8/10; legge 132/2025 6,9/10; esito integrato 6,9/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

L'Ucraina combina una forte accelerazione della digitalizzazione pubblica e capacità cyber sviluppate in condizioni di guerra con un'esposizione eccezionale ad attacchi, interruzioni fisiche, dislocazione di infrastrutture e dipendenza da supporto esterno. La cooperazione con l'Italia ha rilevanza strategica e politica, ma richiede architetture resilienti, backup geografici, gestione del rischio bellico e separazione tra attività civili, governative e dual-use. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 51/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (6,6/10) e indice FOTR (6,7/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Amministrazione digitale avanzata e forte resilienza cyber, inserite in un contesto bellico che impone ridondanza, continuità fuori area e segregazione dei dati più sensibili.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	82,5% / 21,7 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 9.937 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	88,4 / 86,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	83,9/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	64,6/100 - rank 41	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza
Libertà digitale	Freedom on the Net / Freedom in the World	62/100 - Parzialmente libero / Parzialmente libero (51/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	8,5 / 4,5 / 7,2	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Ucraina, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Ucraina le evidenze principali sono GTMI 86,6/100, EGDI 88,4/100, GCI 83,9/100, AI readiness 64,6/100. La dimensione più robusta è maturità infrastrutturale (7,5/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,2/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Ucraina è 7,5/10. La base statistica rileva utenti Internet pari al 82,5% nel 2024; 21,7 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 9.937 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Ucraina al posto 41 con un valore medio di 64,6/100; il pilastro migliore è governance (83,0/100), quello più debole è sviluppo e diffusione (40,3/100). Il GTMI 2025 è 86,6/100. Il punteggio S2 è 7,2/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Ucraina è valutata sufficiente ma disomogenea, con S3 pari a 6,9/10. Le evidenze disponibili comprendono indice UN di capitale umano 82,4/100, sviluppo e diffusione dell'IA 40,3/100, penetrazione Internet 82,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Ucraina ottiene S4 5,2/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Ucraina, Ecosistema nazionale con forte sostegno e fornitura da Stati Uniti, Unione europea e altri alleati; alta integrazione di soluzioni dual-use. L'impatto sulla valutazione è misurato da S4=5,2/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Ucraina è S5 6,4/10. La base ITU registra ITU GCI 83,9/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (14,6/20). Freedom on the Net è 62/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (51/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Legge nazionale sulla protezione dei dati, architettura Diia e progressivo allineamento UE; il contesto bellico impone misure speciali di continuità e resilienza.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	8,5	Crimini finanziari	7,0
Reti criminali	7,5	Attori incorporati nello Stato	8,0
Attori stranieri	7,0	Attori del settore privato	5,0
Resilienza complessiva	4,5	Cooperazione internazionale	7,5
Politiche e norme nazionali	4,5	Forze dell'ordine	5,0
Antiriciclaggio	4,5	Prevenzione	4,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	7,2 - ALTO

Pressione del crimine digitale. Il profilo di Ucraina restituisce un rischio FOTR-CY di 7,2/10 (alto). La componente cyber-dipendente vale 8,5/10 e quella finanziaria 7,0/10; la risposta sistemica è valutata debole, con resilienza media di 4,5/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e reti criminali (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Ucraina assumono particolare rilevanza ransomware come servizio, malware sottrattori di informazioni, infrastrutture di hosting permissive, DDoS, furto di credenziali, estorsione dei dati e possibili sovrapposizioni tra criminalità professionale e finalità geopolitiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Ucraina, la resilienza complessiva è debole (4,5/10); la cooperazione internazionale è robusta (7,5/10), le politiche e norme nazionali sono deboli (4,5/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 4,5/10, prevenzione 4,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Ucraina, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; blocco di hosting e ASN ad alta reputazione negativa, ricerca proattiva delle minacce su malware sottrattori di informazioni e controllo dei canali RDP/VPN; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Ucraina. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Ucraina, In Ucraina le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Ucraina, Il livello governativo di Ucraina presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Ucraina, Sul piano militare e dual-use, Ucraina mostra stretta cooperazione con ecosistemi occidentali e capacità dual-use significative. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Ucraina, Legge nazionale sulla protezione dei dati, architettura Diia e progressivo allineamento UE; il contesto bellico impone misure speciali di continuità e resilienza. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Ucraina, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 5,6/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
7,5	7,2	6,9	5,2	6,4	6,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,1	5,8	6,0	8,2	6,2	5,6

Il GCRI di Ucraina è 6,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 6,7/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (8,2/10), mentre il più basso è Trasferibilità dati (5,6/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio	Medio	Medio	Medio

La matrice applica il FOTR di 6,7/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Ucraina, la cautela si concentra su 6 ambiti a rischio intermedio: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Ucraina, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Ucraina, Dal punto di vista italiano, Ucraina rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. La cooperazione con Ucraina è favorevole ma condizionata: il valore FOTR di 6,7/10 richiede clausole mirate su dati, subfornitura, audit e continuità, soprattutto rispetto a Trasferibilità dati.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.

Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

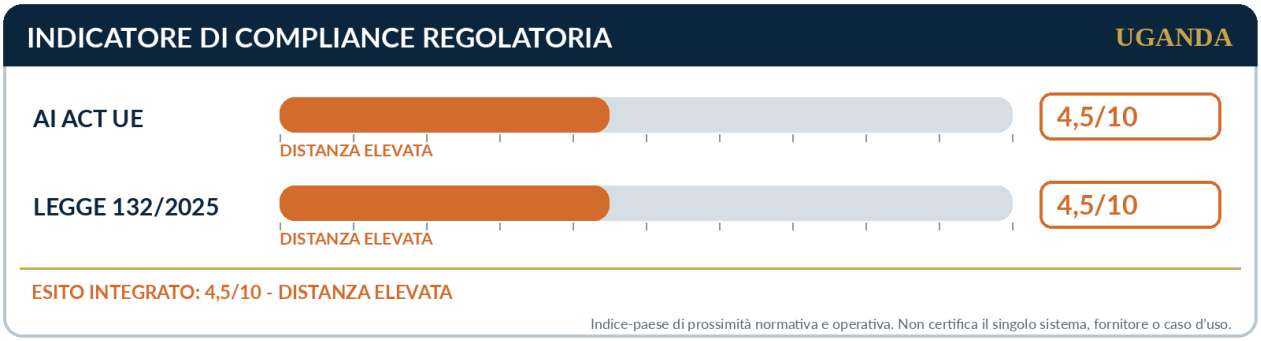
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Ucraina: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Uganda

Posizione FOTR	155	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	4,5	GCRI / 10	4,5	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Uganda, AI Act UE 4,5/10; legge 132/2025 4,5/10; esito integrato 4,5/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Uganda, situato in Africa orientale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 33/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (4,5/10) e indice FOTR (4,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per Uganda non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	8,9% / 0,2 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	55,3% / 54 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	44,6 / 79,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	82,9/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	36,2/100 - rank 113	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	52/100 - Parzialmente libero / Non libero (33/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	6,0 / 3,7 / 6,7	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Uganda, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Uganda le evidenze principali sono GTMI 79,2/100, EGDI 44,6/100, GCI 82,9/100, AI readiness 36,2/100. La dimensione più robusta è postura di sicurezza cyber (6,5/10), mentre la criticità relativa riguarda maturità infrastrutturale (2,1/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Uganda è 2,1/10. La base statistica rileva utenti Internet pari al 8,9% nel 2024; 0,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 55,3% nel 2024; 54 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Uganda al posto 113 con un valore medio di 36,2/100; il pilastro migliore è adozione pubblica (70,8/100), quello più debole è politiche pubbliche (12,0/100). Il GTMI 2025 è 79,2/100. Il punteggio S2 è 4,8/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Uganda è valutata fragile, con S3 pari a 4,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 50,2/100, sviluppo e diffusione dell'IA 20,9/100, penetrazione Internet 8,9%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Uganda ottiene S4 5,0/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Uganda, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=5,0/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Uganda è S5 6,5/10. La base ITU registra ITU GCI 82,9/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (13,6/20). Freedom on the Net è 52/100 - Parzialmente libero, mentre Freedom in the World è Non libero (33/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	6,0	Crimini finanziari	7,5
Reti criminali	7,0	Attori incorporati nello Stato	8,0
Attori stranieri	7,0	Attori del settore privato	6,5
Resilienza complessiva	3,7	Cooperazione internazionale	5,0
Politiche e norme nazionali	5,0	Forze dell'ordine	3,0
Antiriciclaggio	3,5	Prevenzione	4,0
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	6,7 - ALTO

Pressione del crimine digitale. Il profilo di Uganda restituisce un rischio FOTR-CY di 6,7/10 (alto). La componente cyber-dipendente vale 6,0/10 e quella finanziaria 7,5/10; la risposta sistemica è valutata debole, con resilienza media di 3,7/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e reti criminali (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Uganda assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Uganda, la resilienza complessiva è debole (3,7/10); la cooperazione internazionale è debole (5,0/10), le politiche e norme nazionali sono deboli (5,0/10) e la capacità delle forze dell'ordine è molto debole (3,0/10). Completano il quadro antiriciclaggio 3,5/10, prevenzione 4,0/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Uganda, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Uganda. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Uganda, In Uganda le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Uganda, Il livello governativo di Uganda presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. L'affidabilità deve essere verificata per singolo ente: la media nazionale non sostituisce l'esame della piattaforma, del contratto e del fornitore effettivo.

Tecnologie militari e dual-use. Per Uganda, Sul piano militare e dual-use, Uganda mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Uganda, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Uganda, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,3/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
2,1	4,8	4,1	5,0	6,5	4,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,6	4,6	4,1	4,9	4,2	4,3

Il GCRI di Uganda è 4,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (4,9/10), mentre il più basso è Trasparenza istituzionale (4,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Uganda, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Uganda, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Uganda, Dal punto di vista italiano, Uganda rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Uganda ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

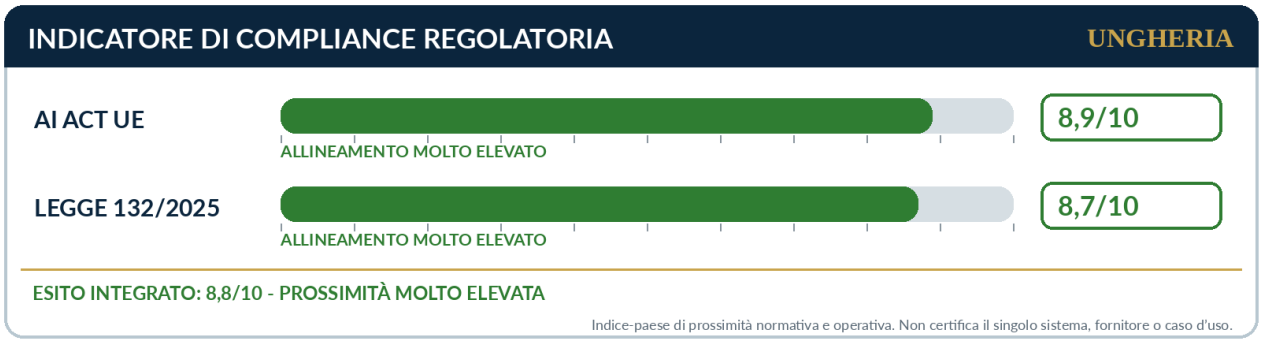
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Uganda: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Ungheria

Posizione FOTR	40	**Area**	Europa	**Subregione**	Europa occidentale e centrale
Status	Stato membro delle Nazioni Unite	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	7/7 famiglie
FOTR / 10	8,0	**GCRI / 10**	7,5	**Classe operativa**	**Affidabilità alta**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Ungheria, AI Act UE 8,9/10; legge 132/2025 8,7/10; esito integrato 8,8/10, classe «Allineamento molto elevato». Il Paese è inserito nel perimetro normativo dell'Unione: la prossimità istituzionale è elevata, ma la conformità resta riferita al singolo sistema, al ruolo dell'operatore e alla classe di rischio. Sono normalmente sostenibili procedure ordinarie rafforzate: classificazione del sistema, documentazione tecnica, gestione del rischio, logging, supervisione umana, cybersecurity e verifica dei subfornitori.

Premessa geopolitica e tecnologica

Per un operatore italiano, Ungheria non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. L'appartenenza simultanea all'Unione europea e alla NATO colloca il Paese nello spazio giuridico del mercato digitale europeo e nell'architettura di sicurezza euro-atlantica. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 65/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,5/10) e indice FOTR (8,0/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Ungheria combina buona maturità tecnologica e relativa prevedibilità normativa. Il livello di rischio aumenta nei progetti che coinvolgono dati sanitari, identità, infrastrutture critiche o ricerca strategica.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	93,8% / 37,5 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 55.077 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	80,4 / 85,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	88,7/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	66,2/100 - rank 35	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	69/100 - Parzialmente libero / Parzialmente libero (65/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Regime intra-SEE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	5,5 / 4,8 / 5,6	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Ungheria, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Ungheria le evidenze principali sono GTMI 85,4/100, EGDI 80,4/100, GCI 88,7/100, AI readiness 66,2/100. La dimensione più robusta è maturità infrastrutturale (9,1/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,0/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Ungheria è 9,1/10. La base statistica rileva utenti Internet pari al 93,8% nel 2024; 37,5 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 55.077 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Ungheria al posto 35 con un valore medio di 66,2/100; il pilastro migliore è adozione pubblica (82,6/100), quello più debole è sviluppo e diffusione (45,2/100). Il GTMI 2025 è 85,4/100. Il punteggio S2 è 7,0/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Ungheria è valutata sufficiente ma disomogenea, con S3 pari a 7,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 87,0/100, sviluppo e diffusione dell'IA 45,2/100, penetrazione Internet 93,8%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Ungheria ottiene S4 6,0/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Italia/UE, Stati Uniti; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Ungheria, Ecosistema europeo e nazionale, con forte presenza statunitense nel cloud e nel software e componentistica globale. La verifica preventiva deve distinguere sede contrattuale, controllo societario,

luogo del supporto e origine dei componenti. L'impatto sulla valutazione è misurato da S4=6,0/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Ungheria è S5 8,0/10. La base ITU registra ITU GCI 88,7/100, Tier 2 - avanzato; il pilastro relativamente più debole è sviluppo delle capacità (12,6/20). Freedom on the Net è 69/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (65/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: GDPR, normativa nazionale su privacy e sicurezza informatica; applicazione del diritto UE, con attenzione agli accessi pubblici e all'indipendenza dei controlli.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	5,5	Crimini finanziari	6,5
Reti criminali	4,0	Attori incorporati nello Stato	7,5
Attori stranieri	5,5	Attori del settore privato	5,5
Resilienza complessiva	4,8	Cooperazione internazionale	4,0
Politiche e norme nazionali	5,5	Forze dell'ordine	5,0
Antiriciclaggio	5,5	Prevenzione	6,0
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	5,6 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (5,5/10), criminalità finanziaria (6,5/10) e resilienza (4,8/10) colloca Ungheria in una fascia di rischio significativo, pari a 5,6/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,5/10) e attori stranieri (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Ungheria assumono particolare rilevanza ransomware, estorsione mediante sottrazione o cifratura dei dati, attacchi alla supply chain, compromissione delle caselle di posta aziendale, malware sottrattori di informazioni, furto d'identità e riciclaggio tramite servizi finanziari e cripto-attività. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Ungheria, la resilienza complessiva è debole (4,8/10); la cooperazione internazionale è debole (4,0/10), le politiche e norme nazionali sono intermedie (5,5/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 6,0/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Ungheria, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Ungheria. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Ungheria, In Ungheria le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Ungheria, Il livello governativo di Ungheria presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Ungheria, Sul piano militare e dual-use, Ungheria mostra integrazione con standard e cooperazione NATO, pur con capacità nazionali e dipendenze industriali differenti. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Ungheria, GDPR, normativa nazionale su privacy e sicurezza informatica; applicazione del diritto UE, con attenzione agli accessi pubblici e all'indipendenza dei controlli. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Ungheria, Flussi dall'Italia normalmente in regime intra-SEE, nel rispetto di GDPR, minimizzazione, sicurezza, accountability e regole settoriali. Non è comunque sufficiente la sola localizzazione geografica: occorre verificare sub-responsabili, accessi remoti e catena cloud. La componente FOTR di trasferibilità è 9,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,1	7,0	7,4	6,0	8,0	7,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,6	7,4	7,2	8,6	7,3	9,0

Il GCRI di Ungheria è 7,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (9,0/10), mentre il più basso è Trasparenza istituzionale (7,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Ungheria, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Ungheria, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Ungheria, Dal punto di vista italiano, Ungheria rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Ungheria, il FOTR di 8,0/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (7,2/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.

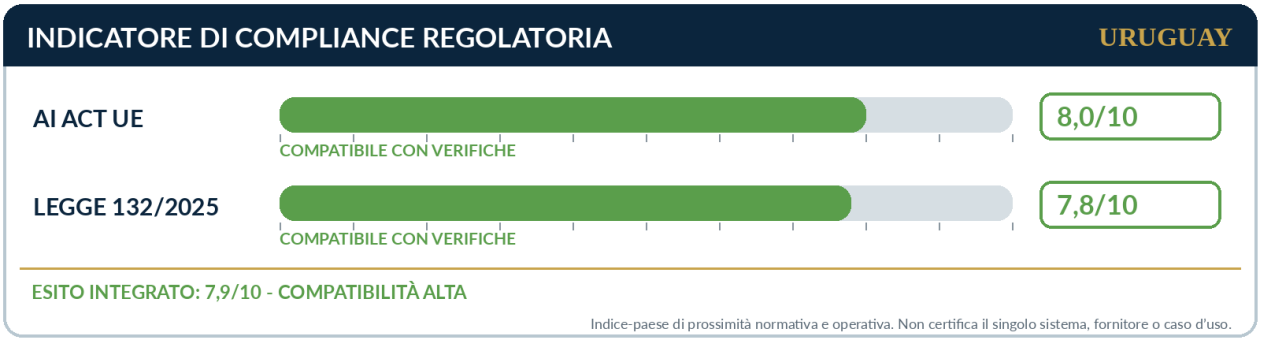
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Ungheria: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Uruguay

Posizione FOTR	41	Area	Americhe	Subregione	America meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	8,0	GCRI / 10	7,6	Classe operativa	Affidabilità alta

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Uruguay, AI Act UE 8,0/10; legge 132/2025 7,8/10; esito integrato 7,9/10, classe «Compatibile con verifiche». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Prima dell'ingaggio occorre una analisi degli scostamenti mirata su trasparenza, governance dei dati, rappresentanza nell'UE, audit e rimedi contrattuali.

Premessa geopolitica e tecnologica

Uruguay è stato membro delle nazioni unite collocato in America meridionale. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 97/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (7,6/10) e indice FOTR (8,0/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Uruguay combina buona maturità tecnologica e relativa prevedibilità normativa. Il livello di rischio aumenta nei progetti che coinvolgono dati sanitari, identità, infrastrutture critiche o ricerca strategica.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	92,0% / 33,0 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 4.641 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	90,1 / 90,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	94,7/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	61,5/100 - rank 55	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (97/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Adeguatezza UE / Firmatario/invitato	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 7,5 / 3,8	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Uruguay, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Uruguay le evidenze principali sono GTMI 90,8/100, EGDI 90,1/100, GCI 94,7/100, AI readiness 61,5/100. La dimensione più robusta è maturità infrastrutturale (9,0/10), mentre la criticità relativa riguarda indipendenza della supply chain (6,1/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Uruguay è 9,0/10. La base statistica rileva utenti Internet pari al 92,0% nel 2024; 33,0 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 4.641 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Uruguay al posto 55 con un valore medio di 61,5/100; il pilastro migliore è governance (84,5/100), quello più debole è sviluppo e diffusione (31,2/100). Il GTMI 2025 è 90,8/100. Il punteggio S2 è 7,0/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Uruguay è valutata sufficiente ma disomogenea, con S3 pari a 7,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 87,5/100, sviluppo e diffusione dell'IA 31,2/100, penetrazione Internet 92,0%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Uruguay ottiene S4 6,1/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Uruguay, Mercato generalmente integrato con Stati Uniti ed Europa, con presenza crescente di gruppi cinesi nelle telecomunicazioni e nell'hardware e capacità locali nei servizi software. L'impatto sulla

valutazione è misurato da S4=6,1/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Uruguay è S5 8,8/10. La base ITU registra ITU GCI 94,7/100, Tier 2 - avanzato; il pilastro relativamente più debole è cooperazione (16,6/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (97/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Firmatario/invitato. Quadro normativo sintetico: Ley 18.331 e sistema di supervisione; decisione UE di adeguatezza e buona interoperabilità giuridica regionale.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	4,0
Reti criminali	4,5	Attori incorporati nello Stato	3,5
Attori stranieri	4,0	Attori del settore privato	3,5
Resilienza complessiva	7,5	Cooperazione internazionale	9,0
Politiche e norme nazionali	7,0	Forze dell'ordine	7,5
Antiriciclaggio	6,5	Prevenzione	6,5
Supporto vittime e testimoni	7,5	Rischio operativo FOTR-CY	3,8 - MODERATO

Quadro criminale digitale. Per Uruguay, l'indice operativo FOTR-CY è 3,8/10, classe moderata. Il mercato dei reati cyber-dipendenti è intermedio (4,5/10), mentre i crimini finanziari sono intermedi (4,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (4,5/10) e attori stranieri (4,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Uruguay assumono particolare rilevanza trojan bancari e malware per dispositivi mobili, ransomware, compromissione delle caselle di posta aziendale, frodi con cripto-attività, estorsione digitale e attacchi a enti pubblici, sanità, servizi finanziari e filiere logistiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Uruguay, la resilienza complessiva è intermedia (7,5/10); la cooperazione internazionale è robusta (9,0/10), le politiche e norme nazionali sono intermedie (7,0/10) e la capacità delle forze dell'ordine è robusta (7,5/10). Completano il quadro antiriciclaggio 6,5/10, prevenzione 6,5/10 e supporto a vittime e testimoni 7,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Uruguay, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Uruguay. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Uruguay, In Uruguay le tecnologie destinate alla popolazione mostrano ampia diffusione di smartphone, servizi online, pagamenti elettronici e piattaforme internazionali o nazionali. Per i partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Uruguay, Il livello governativo di Uruguay presenta programmi di e-government strutturati e un uso crescente di cloud, identità digitale e dati amministrativi. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Uruguay, Sul piano militare e dual-use, Uruguay mostra cooperazione internazionale e capacità dual-use selettive, spesso basate su più fornitori. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Uruguay, Ley 18.331 e sistema di supervisione; decisione UE di adeguatezza e buona interoperabilità giuridica regionale. Lo stato rispetto alla Convenzione di Budapest è: Firmatario/invitato; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Uruguay, È disponibile una decisione UE di adeguatezza. L'operatore italiano deve comunque controllare la portata della decisione, i trasferimenti successivi, le misure di sicurezza e le eventuali discipline settoriali. La componente FOTR di trasferibilità è 10,0/10 e il rischio sui dati personali è Basso; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
9,0	7,0	7,1	6,1	8,8	7,6

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
8,3	8,1	6,9	7,3	7,6	10,0

Il GCRI di Uruguay è 7,6/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 8,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Trasferibilità dati (10,0/10), mentre il più basso è Trasparenza istituzionale (6,9/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso	Medio-basso

La matrice applica il FOTR di 8,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Uruguay, la cautela si concentra su 5 ambiti a rischio intermedio: Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Uruguay, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Uruguay, Dal punto di vista italiano, Uruguay rientra nella classe «Affidabilità alta»: cooperazione favorevole ma non automatica, subordinata a verifica settoriale, trasferimenti documentati e controllo delle dipendenze tecnologiche. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Uruguay, il FOTR di 8,0/10 consente una cooperazione ordinaria controllata; il presidio prioritario resta Trasparenza istituzionale (6,9/10), con verifica del fornitore, monitoraggio e diritto di uscita.

Presidi minimi raccomandati

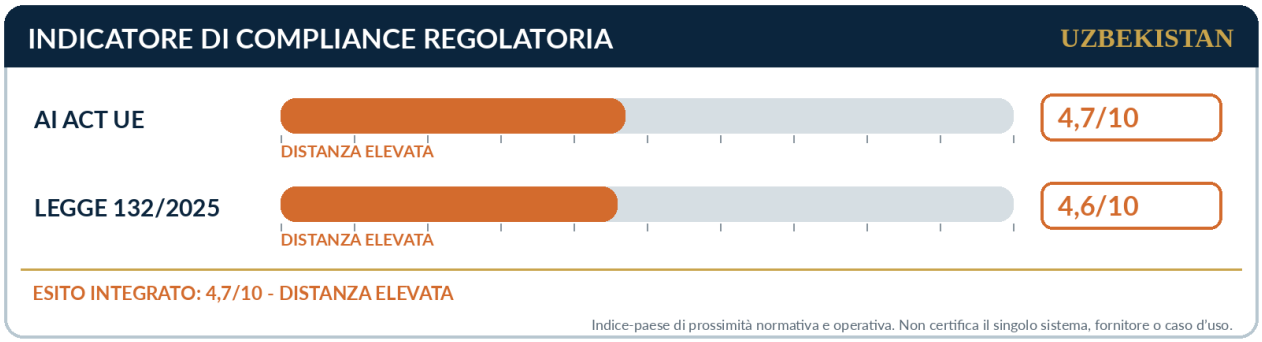
Mappare titolare, responsabili, sub-responsabili, assistenza remota e Paesi di transito.
Prevedere cifratura, gestione degli accessi privilegiati, logging e notifica tempestiva degli incidenti.
Inserire audit, portabilità, restituzione/cancellazione e piano di uscita verificabile.
Documentare la base del trasferimento e verificare eventuali eccezioni di sicurezza nazionale.

Profilo Celeborn Intelligence di Uruguay: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Uzbekistan

Posizione FOTR	156	Area	Asia	Subregione	Caucaso e Asia centrale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	4,5	GCRI / 10	6,7	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Uzbekistan, AI Act UE 4,7/10; legge 132/2025 4,6/10; esito integrato 4,7/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Nel quadro di Asia, Uzbekistan presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina, Russia, Giappone/Corea. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 12/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (6,7/10) è superiore al punteggio FOTR (4,5/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Uzbekistan presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	89,5% / 34,7 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 967 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	80,0 / 95,8	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	89,2/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	58,8/100 - rank 62	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	29/100 - Non libero / Non libero (12/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	3,0 / 3,8 / 5,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Uzbekistan, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Uzbekistan le evidenze principali sono GTMI 95,8/100, EGDI 80,0/100, GCI 89,2/100, AI readiness 58,8/100. La dimensione più robusta è maturità infrastrutturale (8,6/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,4/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Uzbekistan è 8,6/10. La base statistica rileva utenti Internet pari al 89,5% nel 2024; 34,7 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 967 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Uzbekistan al posto 62 con un valore medio di 58,8/100; il pilastro migliore è politiche pubbliche (80,5/100), quello più debole è resilienza (38,0/100). Il GTMI 2025 è 95,8/100. Il punteggio S2 è 6,7/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Uzbekistan è valutata sufficiente ma disomogenea, con S3 pari a 6,3/10. Le evidenze disponibili comprendono indice UN di capitale umano 75,8/100, sviluppo e diffusione dell'IA 43,8/100, penetrazione Internet 89,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Uzbekistan ottiene S4 5,4/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Cina, Russia, Giappone/Corea; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Uzbekistan, Mercato misto con forte presenza cinese, russa e coreana, oltre a fornitori occidentali in progetti selettivi. L'impatto sulla valutazione è misurato da S4=5,4/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Uzbekistan è S5 6,4/10. La base ITU registra ITU GCI 89,2/100, Tier 2 - avanzato; il pilastro relativamente più debole è organizzazione (15,8/20). Freedom on the Net è 29/100 - Non libero, mentre Freedom in the World è Non libero (12/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Legge sui dati personali e requisiti di localizzazione; riforme digitali rapide, ma rimedi e trasparenza ancora limitati.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	3,0	Crimini finanziari	6,0
Reti criminali	5,0	Attori incorporati nello Stato	7,0
Attori stranieri	5,0	Attori del settore privato	5,5
Resilienza complessiva	3,8	Cooperazione internazionale	4,0
Politiche e norme nazionali	4,0	Forze dell'ordine	3,5
Antiriciclaggio	4,0	Prevenzione	4,5
Supporto vittime e testimoni	4,0	Rischio operativo FOTR-CY	5,0 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Uzbekistan il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 5,0/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 3,0/10; le frodi e i reati finanziari 6,0/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (7,0/10) e attori del settore privato (5,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Uzbekistan assumono particolare rilevanza ransomware come servizio, malware sottrattori di informazioni, infrastrutture di hosting permissive, DDoS, furto di credenziali, estorsione dei dati e possibili sovrapposizioni tra criminalità professionale e finalità geopolitiche. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Uzbekistan, la resilienza complessiva è debole (3,8/10); la cooperazione internazionale è debole (4,0/10), le politiche e norme nazionali sono deboli (4,0/10) e la capacità delle forze dell'ordine è debole (3,5/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 4,5/10 e supporto a vittime e testimoni 4,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Uzbekistan, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; blocco di hosting e ASN ad alta reputazione negativa, ricerca proattiva delle minacce su malware sottrattori di informazioni e controllo dei canali RDP/VPN; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Uzbekistan. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Uzbekistan, In Uzbekistan le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La

superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Uzbekistan, Il livello governativo di Uzbekistan presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Uzbekistan, Sul piano militare e dual-use, Uzbekistan mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Uzbekistan, Legge sui dati personali e requisiti di localizzazione; riforme digitali rapide, ma rimedi e trasparenza ancora limitati. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Uzbekistan, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,1/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,6	6,7	6,3	5,4	6,4	6,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,6	4,9	4,1	4,5	4,8	4,1

Il GCRI di Uzbekistan è 6,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (4,9/10), mentre il più basso è Trasparenza istituzionale (4,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Uzbekistan, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Uzbekistan, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Uzbekistan, Dal punto di vista italiano, Uzbekistan rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Uzbekistan ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

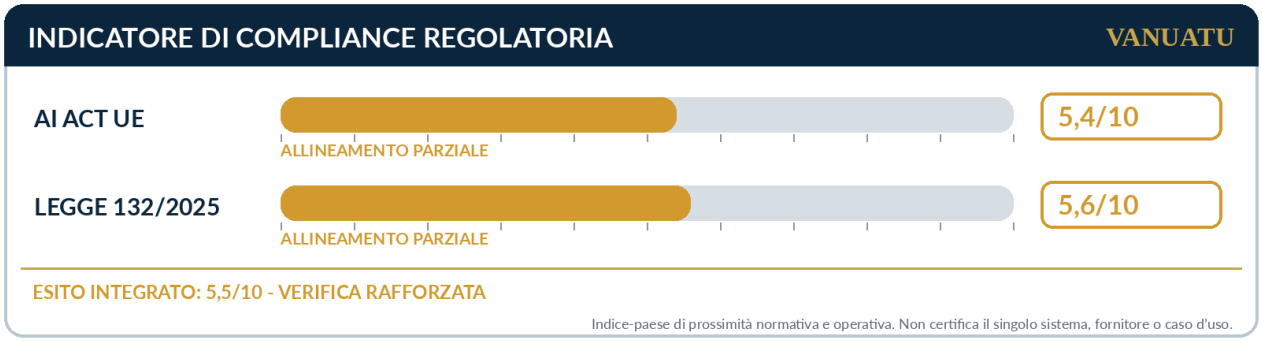
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Uzbekistan: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Vanuatu

Posizione FOTR	112	Area	Oceania	Subregione	Pacifico insulare
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	5,6	GCRI / 10	4,5	Classe operativa	Affidabilità selettiva

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Vanuatu, AI Act UE 5,4/10; legge 132/2025 5,6/10; esito integrato 5,5/10, classe «Allineamento parziale». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. L'allineamento è parziale: servono clausole sostanziali, controllo italiano delle chiavi e dei log, segregazione degli ambienti e prova documentale dei requisiti.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Vanuatu, situato in Pacifico insulare, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La distanza geografica e l'insularità rendono centrali cavi sottomarini, satelliti, continuità energetica e dipendenza da fornitori australiani, neozelandesi, statunitensi o asiatici. Il territorio è classificato come insulare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Ecosistema estero o regionale da verificare per singolo appalto. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è libero con 82/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (5,6/10) supera il GCRI tecnico (4,5/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Vanuatu dispone di un ecosistema digitale in sviluppo, con opportunità concrete ma livelli di capacità non omogenei. La cooperazione italiana è possibile selezionando controparti, dati e architetture, evitando affidamenti indistinti.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	22,4% / 1,2 per 100	2015/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	65,5% / 1.919 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	54,3 / 41,4	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	69,3/100 - Tier 3 - in consolidamento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	28,3/100 - rank 132	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Libero (82/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Parte	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,5 / 4,9 / 3,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Vanuatu, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Vanuatu le evidenze principali sono GTMI 41,4/100, EGDI 54,3/100, GCI 69,3/100, AI readiness 28,3/100. La dimensione più robusta è postura di sicurezza cyber (6,3/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,4/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Vanuatu è 4,3/10. La base statistica rileva utenti Internet pari al 22,4% nel 2015; 1,2 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 65,5% nel 2024; 1.919 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come adozione selettiva: copertura mobile utile ma capacità fissa, ridondanza o continuità restano disomogenee. L'insularità rende essenziali cavi sottomarini, stazioni di approdo, capacità satellitare di riserva e scorte tecniche; un'elevata copertura utente può coesistere con pochi punti fisici di guasto. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Vanuatu al posto 132 con un valore medio di 28,3/100; il pilastro migliore è resilienza (44,6/100), quello più debole è politiche pubbliche (15,5/100). Il GTMI 2025 è 41,4/100. Il punteggio S2 è 3,4/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Vanuatu è valutata fragile, con S3 pari a 4,1/10. Le evidenze disponibili comprendono indice UN di capitale umano 53,5/100, sviluppo e diffusione dell'IA 20,6/100, penetrazione Internet 22,4%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Vanuatu ottiene S4 4,4/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Ecosistema estero o regionale da verificare per singolo appalto; l'indicatore di indipendenza disponibile è 4,1/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Vanuatu, Dipendenza da Australia, Nuova Zelanda, Stati Uniti, Francia e operatori satellitari o sottomarini; la scala ridotta limita la diversificazione e aumenta il rischio di concentrazione. L'impatto sulla

valutazione è misurato da S4=4,4/10 e dal proxy di indipendenza 4,1/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Vanuatu è S5 6,3/10. La base ITU registra ITU GCI 69,3/100, Tier 3 - in consolidamento; il pilastro relativamente più debole è sviluppo delle capacità (5,6/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Libero (82/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Parte. Quadro normativo sintetico: Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,5	Crimini finanziari	3,5
Reti criminali	1,5	Attori incorporati nello Stato	3,0
Attori stranieri	4,0	Attori del settore privato	1,5
Resilienza complessiva	4,9	Cooperazione internazionale	5,5
Politiche e norme nazionali	6,0	Forze dell'ordine	6,5
Antiriciclaggio	2,5	Prevenzione	3,0
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	3,4 - MODERATO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (2,5/10), criminalità finanziaria (3,5/10) e resilienza (4,9/10) colloca Vanuatu in una fascia di rischio moderato, pari a 3,4/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (4,0/10) e attori incorporati nello Stato (3,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Vanuatu assumono particolare rilevanza ransomware e violazioni di enti pubblici o sanitari, compromissione delle caselle di posta aziendale, phishing, furto d'identità e dipendenza da capacità investigative, cloud e telecomunicazioni esterne. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Vanuatu, la resilienza complessiva è debole (4,9/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è intermedia (6,5/10). Completano il quadro antiriciclaggio 2,5/10, prevenzione 3,0/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Vanuatu, il livello moderato non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Vanuatu. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Vanuatu, In Vanuatu le tecnologie destinate alla popolazione mostrano crescita rapida di connettività mobile, fintech e servizi digitali, con divari territoriali o sociali ancora visibili. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Vanuatu, Il livello governativo di Vanuatu presenta piattaforme pubbliche in espansione, spesso accompagnate da progetti di identità digitale, registri elettronici e cloud governativo. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Vanuatu, Sul piano militare e dual-use, Vanuatu mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Vanuatu, Normativa privacy e cyber spesso di piccola scala, integrata da standard regionali e assistenza di Australia o Nuova Zelanda; capacità locale e dipendenza da fornitori esterni devono essere valutate. Lo stato rispetto alla Convenzione di Budapest è: Parte; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Vanuatu, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 5,4/10 e il rischio sui dati personali è Medio; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
4,3	3,4	4,1	4,4	6,3	4,5

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,9	4,9	5,7	6,7	4,5	5,4

Il GCRI di Vanuatu è 4,5/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 5,6/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (6,7/10), mentre il più basso è Supply chain (4,5/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio	Medio	Medio-alto	Medio-alto	Medio	Medio

La matrice applica il FOTR di 5,6/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Vanuatu, 2 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Cloud e infrastrutture, IP e R&S. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Vanuatu, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Vanuatu, Dal punto di vista italiano, Vanuatu rientra nella classe «Cooperazione selettiva»: cooperazione selettiva, subordinata a limitazione delle categorie di dati, TIA, audit, cifratura e separazione degli ambienti. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Vanuatu è indicata una cooperazione selettiva, coerente con il FOTR di 5,6/10: limitare privilegi e categorie di dati, evitare dipendenze irreversibili e sottoporre Cloud e infrastrutture a decisione caso per caso.

Presidi minimi raccomandati

Applicare SCC/BCR quando necessarie e redigere un Transfer Impact Assessment specifico.
Limitare dati e funzioni, separando ambienti ordinari, sensibili e strategici.
Mantenere chiavi, backup e capacità di amministrazione sotto controllo italiano o SEE.

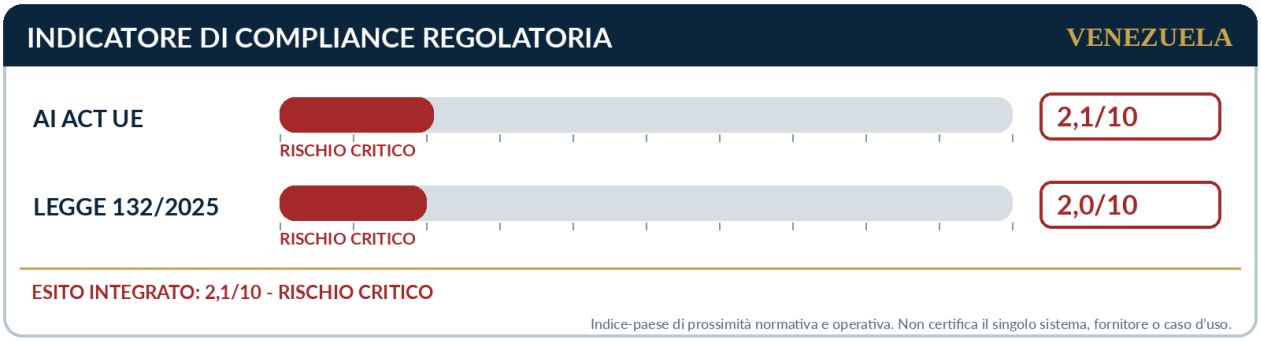
Eseguire audit periodici su fornitore, subfornitura, continuità e rimedi locali.

Profilo Celeborn Intelligence di Vanuatu: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Venezuela

Posizione FOTR	190	Area	Americhe	Subregione	America meridionale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	6/7 famiglie
FOTR / 10	2,0	GCRI / 10	4,0	Classe operativa	Rischio estremo

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Venezuela, AI Act UE 2,1/10; legge 132/2025 2,0/10; esito integrato 2,1/10, classe «Rischio critico». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. Il rischio è critico: evitare sistemi ad alto rischio o funzioni essenziali, usare esclusivamente ambienti isolati e dati sintetici, con autorizzazione istituzionale preventiva.

Premessa geopolitica e tecnologica

Per un operatore italiano, Venezuela non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. Il continente presenta integrazione con ecosistemi statunitensi e differenze profonde tra regimi di protezione dei dati, capacità pubbliche e resilienza delle infrastrutture. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Cina, Russia. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 13/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (4,0/10) è superiore al punteggio FOTR (2,0/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. Il rapporto digitale con Venezuela deve essere considerato eccezionale e ad alta esposizione. Sono necessari screening sanzionatori, autorizzazioni, segregazione completa e impossibilità tecnica di accedere ai dati in chiaro.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	76,7% / 12,9 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 247 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	53,6 / 34,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	30,4/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	25,5/100 - rank 145	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (13/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 1,9 / 7,0	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Venezuela, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Venezuela le evidenze principali sono GTMI 34,2/100, EGDI 53,6/100, GCI 30,4/100, AI readiness 25,5/100. La dimensione più robusta è maturità infrastrutturale (6,0/10), mentre la criticità relativa riguarda postura di sicurezza cyber (2,9/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Venezuela è 6,0/10. La base statistica rileva utenti Internet pari al 76,7% nel 2024; 12,9 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 247 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come fase di espansione della banda larga e del 5G, con differenze territoriali da verificare. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Venezuela al posto 145 con un valore medio di 25,5/100; il pilastro migliore è infrastrutture IA (39,6/100), quello più debole è sviluppo e diffusione (12,8/100). Il GTMI 2025 è 34,2/100. Il punteggio S2 è 3,0/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Venezuela è valutata fragile, con S3 pari a 4,0/10. Le evidenze disponibili comprendono indice UN di capitale umano 71,1/100, sviluppo e diffusione dell'IA 12,8/100, penetrazione Internet 76,7%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Venezuela ottiene S4 4,2/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Cina, Russia; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Venezuela, Forte presenza cinese e russa nelle infrastrutture pubbliche, con sistemi occidentali preesistenti e capacità locale limitata. L'impatto sulla valutazione è misurato da S4=4,2/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Venezuela è S5 2,9/10. La base ITU registra ITU GCI 30,4/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è organizzazione (2,2/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (13/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Normativa su dati e telecomunicazioni frammentata, controlli pubblici e sanzioni; elevato rischio di continuità, enforcement e accesso governativo.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	8,0
Reti criminali	5,5	Attori incorporati nello Stato	9,0
Attori stranieri	7,5	Attori del settore privato	6,0
Resilienza complessiva	1,9	Cooperazione internazionale	2,0
Politiche e norme nazionali	2,0	Forze dell'ordine	1,5
Antiriciclaggio	1,5	Prevenzione	2,0
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	7,0 - ALTO

Quadro criminale digitale. Per Venezuela, l'indice operativo FOTR-CY è 7,0/10, classe alta. Il mercato dei reati cyber-dipendenti è intermedio (4,5/10), mentre i crimini finanziari sono molto elevati (8,0/10). Il valore non misura il numero assoluto di denunce: esprime la pervasività stimata dell'economia criminale digitale e deve essere letto insieme alla capacità di rilevazione del Paese.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (9,0/10) e attori stranieri (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Venezuela assumono particolare rilevanza attacchi distruttivi o dimostrativi, compromissione delle telecomunicazioni, furto di credenziali, frodi connesse ad aiuti e identità, DDoS, abuso di infrastrutture scarsamente presidiate e difficoltà di conservazione della prova. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Venezuela, la resilienza complessiva è molto debole (1,9/10); la cooperazione internazionale è molto debole (2,0/10), le politiche e norme nazionali sono molto deboli (2,0/10) e la capacità delle forze dell'ordine è molto debole (1,5/10). Completano il quadro antiriciclaggio 1,5/10, prevenzione 2,0/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Venezuela, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; protezione rafforzata di sistemi bancari, dispositivi mobili, fatturazione elettronica e canali di pagamento; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Venezuela. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Venezuela, In Venezuela le tecnologie destinate alla popolazione mostrano accesso digitale limitato, controllato o discontinuo, con forte dipendenza da reti mobili, piattaforme statali o infrastrutture esterne. La disponibilità del servizio non coincide con la tutela del dato: vanno verificati termini d'uso, cifratura, conservazione e meccanismi di reclamo.

Tecnologie governative e servizi pubblici. Per Venezuela, Il livello governativo di Venezuela presenta capacità amministrativa limitata o fortemente centralizzata, scarsa trasparenza degli appalti e continuità non garantita. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Venezuela, Sul piano militare e dual-use, Venezuela mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Venezuela, Normativa su dati e telecomunicazioni frammentata, controlli pubblici e sanzioni; elevato rischio di continuità, enforcement e accesso governativo. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Venezuela, Non esiste una decisione UE di adeguatezza. SCC o altre garanzie formali possono risultare insufficienti quando accessi pubblici, localizzazione, sanzioni o assenza di rimedi impediscono una protezione sostanzialmente equivalente; per dati sensibili è preferibile evitare il trasferimento. La componente FOTR di trasferibilità è 1,0/10 e il rischio sui dati personali è Estremo; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
6,0	3,0	4,0	4,2	2,9	4,0

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
2,4	3,6	1,1	0,7	3,0	1,0

Il GCRI di Venezuela è 4,0/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 2,0/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (3,6/10), mentre il più basso è Compatibilità strategica (0,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Estremo	Estremo	Alto	Estremo	Estremo	Estremo

La matrice applica il FOTR di 2,0/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Venezuela, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Venezuela, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Venezuela, Dal punto di vista italiano, Venezuela rientra nella classe «Rischio estremo»: presunzione di non cooperazione per attività digitali ordinarie, subordinata a eventuali eccezioni solo per finalità autorizzate, umanitarie o istituzionali, con segregazione completa e chiavi mantenute in Italia. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Per Venezuela, il FOTR di 2,0/10 determina una presunzione di non cooperazione digitale ordinaria; restano possibili soltanto eccezioni autorizzate, umanitarie o istituzionali, integralmente segregate e senza esposizione di Dati personali.

Presidi minimi raccomandati

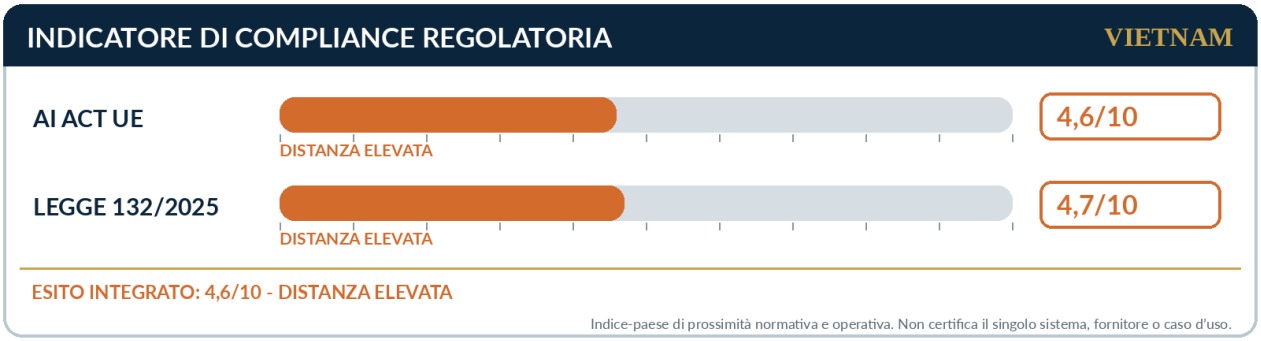
Non trasferire dati italiani sensibili, classificati, strategici o necessari alla continuità di servizi essenziali.
Svolgere verifica sanzionatoria, autorizzativo e reputazionale prima di qualsiasi rapporto.
Per eccezioni autorizzate, usare ambienti segregati, cifratura end-to-end e chiavi custodite in Italia.
Impedire accesso a reti interne, codice sorgente, dataset di addestramento e proprietà intellettuale critica.

Profilo Celeborn Intelligence di Venezuela: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Vietnam

Posizione FOTR	157	Area	Asia	Subregione	Asia sud-orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	4,5	GCRI / 10	6,7	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Vietnam, AI Act UE 4,6/10; legge 132/2025 4,7/10; esito integrato 4,6/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Vietnam è stato membro delle nazioni unite collocato in Asia sud-orientale. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 20/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il GCRI tecnico (6,7/10) è superiore al punteggio FOTR (4,5/10): l'Atlante applica quindi una penalizzazione italiana per fattori giuridici, geopolitici o di trasferibilità dei dati.

Esito sintetico

Quadro sintetico. L'ecosistema digitale di Vietnam è utilizzabile solo con controlli rafforzati. Differenze tra legge formale e prassi, dipendenza da pochi fornitori e capacità cyber variabile aumentano il rischio per un soggetto italiano.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	84,2% / 23,7 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	100,0% / 5.734 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	77,1 / 73,6	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	99,7/100 - Tier 1 - modello di riferimento	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	60,4/100 - rank 45	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	22/100 - Non libero / Non libero (20/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	7,0 / 4,8 / 6,5	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Vietnam, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Vietnam le evidenze principali sono GTMI 73,6/100, EGDI 77,1/100, GCI 99,7/100, AI readiness 60,4/100. La dimensione più robusta è maturità infrastrutturale (8,2/10), mentre la criticità relativa riguarda indipendenza della supply chain (5,4/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Vietnam è 8,2/10. La base statistica rileva utenti Internet pari al 84,2% nel 2024; 23,7 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 100,0% nel 2024; 5.734 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come ecosistema maturo, con reti mobili avanzate e basi adatte al 5G standalone o alla sua estensione. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Vietnam al posto 45 con un valore medio di 60,4/100; il pilastro migliore è governance (88,0/100), quello più debole è resilienza (43,3/100). Il GTMI 2025 è 73,6/100. Il punteggio S2 è 6,4/10 e indica una capacità intermedia. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Vietnam è valutata sufficiente ma disomogenea, con S3 pari a 6,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 72,7/100, sviluppo e diffusione dell'IA 47,0/100, penetrazione Internet 84,2%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Vietnam ottiene S4 5,4/10 e presenta dipendenza gestibile ma significativa. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Vietnam, Forte presenza domestica e asiatica, in particolare cinese, coreana e giapponese; partecipazione statunitense in crescita. L'impatto sulla valutazione è misurato da S4=5,4/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Vietnam è S5 6,9/10. La base ITU registra ITU GCI 99,7/100, Tier 1 - modello di riferimento; il pilastro relativamente più debole è sviluppo delle capacità (19,7/20). Freedom on the Net è 22/100 - Non libero, mentre Freedom in the World è Non libero (20/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Cybersecurity Law, Decree 13/2023 sulla protezione dei dati e obblighi di localizzazione/cooperazione; elevata criticità per dati sensibili e accessi pubblici.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	7,0	Crimini finanziari	7,0
Reti criminali	7,0	Attori incorporati nello Stato	7,0
Attori stranieri	6,5	Attori del settore privato	6,5
Resilienza complessiva	4,8	Cooperazione internazionale	6,0
Politiche e norme nazionali	6,0	Forze dell'ordine	5,0
Antiriciclaggio	5,0	Prevenzione	5,0
Supporto vittime e testimoni	4,5	Rischio operativo FOTR-CY	6,5 - ALTO

Pressione del crimine digitale. Il profilo di Vietnam restituisce un rischio FOTR-CY di 6,5/10 (alto). La componente cyber-dipendente vale 7,0/10 e quella finanziaria 7,0/10; la risposta sistemica è valutata debole, con resilienza media di 4,8/10. L'Atlante usa questi valori per calibrare i presidi contrattuali e tecnici, non per attribuire responsabilità a imprese o istituzioni specifiche.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da reti criminali (7,0/10) e attori incorporati nello Stato (7,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Vietnam assumono particolare rilevanza centri organizzati di truffa, frodi d'investimento e sentimentali, phishing multicanale, batterie di schede SIM, conti prestanome, riciclaggio in cripto-attività e compromissione di servizi esternalizzati. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Vietnam, la resilienza complessiva è debole (4,8/10); la cooperazione internazionale è intermedia (6,0/10), le politiche e norme nazionali sono intermedie (6,0/10) e la capacità delle forze dell'ordine è debole (5,0/10). Completano il quadro antiriciclaggio 5,0/10, prevenzione 5,0/10 e supporto a vittime e testimoni 4,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Vietnam, il livello alto non determina da solo un divieto, ma modifica il perimetro accettabile: monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; uso di dati sintetici o minimizzati e chiavi non disponibili alla controparte; assenza di amministrazione remota non presidiata e approvazione preventiva delle modifiche; verifica sanzionatoria, controllo dell'utilizzatore finale e della destinazione d'uso, nonché escalation istituzionale prima dell'avvio; controllo della filiera contro esposizione a complessi organizzati per truffe telematiche, call center coercitivi e conti prestanome; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Vietnam. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Vietnam, In Vietnam le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La superficie di rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Vietnam, Il livello governativo di Vietnam presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. Nei rapporti con enti italiani vanno chiariti titolarità dei dati, log, sub-responsabili, sede del supporto e poteri di accesso delle autorità.

Tecnologie militari e dual-use. Per Vietnam, Sul piano militare e dual-use, Vietnam mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Vietnam, Cybersecurity Law, Decree 13/2023 sulla protezione dei dati e obblighi di localizzazione/cooperazione; elevata criticità per dati sensibili e accessi pubblici. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Vietnam, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 3,2/10 e il rischio sui dati personali è Alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
8,2	6,4	6,4	5,4	6,9	6,7

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,4	5,5	4,3	4,6	4,8	3,2

Il GCRI di Vietnam è 6,7/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Maturità cyber (5,5/10), mentre il più basso è Trasferibilità dati (3,2/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Vietnam, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Vietnam, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Vietnam, Dal punto di vista italiano, Vietnam rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Vietnam ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

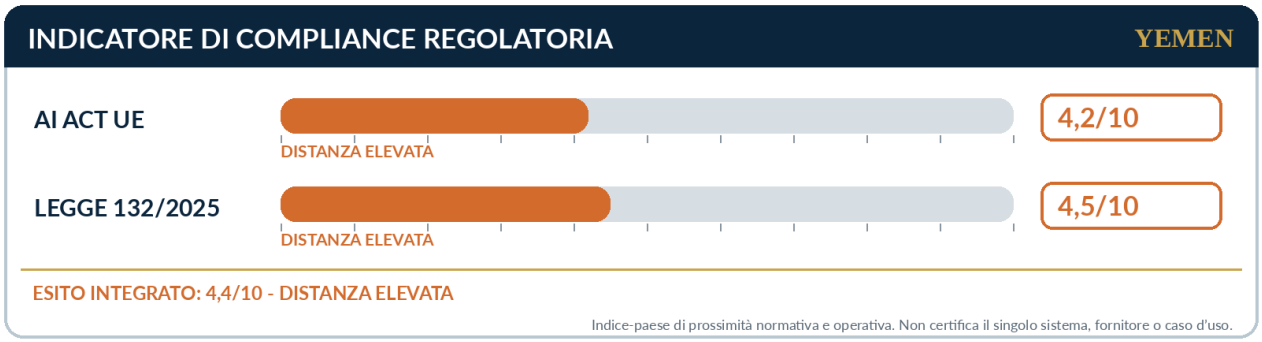
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Vietnam: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Yemen

Posizione FOTR	**158**	**Area**	Asia	**Subregione**	Medio Oriente e Asia occidentale
Status	**Stato membro delle Nazioni Unite**	**Confidenza Celeborn Intelligence**	Alta	**Copertura dati**	6/7 famiglie
FOTR / 10	**4,5**	**GCRI / 10**	**2,2**	**Classe operativa**	**Rischio alto**

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Yemen, AI Act UE 4,2/10; legge 132/2025 4,5/10; esito integrato 4,4/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Nel quadro di Asia, Yemen presenta una posizione geopolitica che incide direttamente sulla scelta di reti, cloud e fornitori. La regione combina grandi poli industriali, ordinamenti fortemente sovrani e catene di fornitura transfrontaliere; l'origine di hardware, firmware e assistenza remota è parte essenziale della valutazione. Il territorio è classificato come costiero; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Stati Uniti, Cina, Giappone/Corea, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 10/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. Il punteggio FOTR (4,5/10) supera il GCRI tecnico (2,2/10), perché prossimità normativa, cooperazione strategica o garanzie sui dati compensano alcune fragilità infrastrutturali.

Esito sintetico

Quadro sintetico. Yemen presenta opportunità di mercato, ma anche criticità significative nella prevedibilità normativa, nella trasparenza degli accessi e nella resilienza. La cooperazione deve essere circoscritta e tecnicamente segregata.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	17,5% / 1,3 per 100	2019/2022	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	86,3% / 15 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	23,2 / 7,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	7,2/100 - Tier 5 - capacità iniziali	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	12,6/100 - rank 191	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	n.d. - Paese non coperto dall'edizione considerata / Non libero (10/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	2,5 / 1,9 / 6,4	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Yemen, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 6/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Yemen le evidenze principali sono GTMI 7,2/100, EGDI 23,2/100, GCI 7,2/100, AI readiness 12,6/100. La dimensione più robusta è indipendenza della supply chain (3,6/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (1,2/10). Sono disponibili 6 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Yemen è 2,3/10. La base statistica rileva utenti Internet pari al 17,5% nel 2019; 1,3 abbonamenti fissi ogni 100 abitanti nel 2022; accesso all'elettricità del 86,3% nel 2024; 15 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. La condizione costiera consente accesso a dorsali internazionali e cavi sottomarini, ma richiede di verificare il numero effettivo di approdi, la diversificazione dei carrier e la separazione geografica dei percorsi. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Yemen al posto 191 con un valore medio di 12,6/100; il pilastro migliore è infrastrutture IA (19,8/100), quello più debole è politiche pubbliche (0,0/100). Il GTMI 2025 è 7,2/100. Il punteggio S2 è 1,2/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Yemen è valutata fragile, con S3 pari a 2,4/10. Le evidenze disponibili comprendono indice UN di capitale umano 26,7/100, sviluppo e diffusione dell'IA 15,4/100, penetrazione Internet 17,5%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Yemen ottiene S4 3,6/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Stati Uniti, Cina, Giappone/Corea, India; l'indicatore di indipendenza disponibile è 4,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Yemen, Ecosistema multi-origine, spesso dominato da fornitori regionali cinesi, giapponesi, coreani, indiani o statunitensi. Per appalti pubblici e reti critiche è necessario identificare controllo societario e

subfornitura. L'impatto sulla valutazione è misurato da S4=3,6/10 e dal proxy di indipendenza 4,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Yemen è S5 1,3/10. La base ITU registra ITU GCI 7,2/100, Tier 5 - capacità iniziali; il pilastro relativamente più debole è organizzazione (0,0/20). Freedom on the Net è n.d. - Paese non coperto dall'edizione considerata, mentre Freedom in the World è Non libero (10/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	2,5	Crimini finanziari	8,0
Reti criminali	7,5	Attori incorporati nello Stato	8,0
Attori stranieri	8,5	Attori del settore privato	6,0
Resilienza complessiva	1,9	Cooperazione internazionale	3,0
Politiche e norme nazionali	2,0	Forze dell'ordine	2,0
Antiriciclaggio	2,0	Prevenzione	1,5
Supporto vittime e testimoni	1,5	Rischio operativo FOTR-CY	6,4 - SIGNIFICATIVO

Sintesi del rischio cybercrime. Yemen presenta un'esposizione stimata significativa (6,4/10): reati cyber-dipendenti 2,5/10, crimini finanziari 8,0/10 e resilienza 1,9/10. Poiché i tre indicatori descrivono fenomeni differenti, il punteggio finale pesa sia il mercato criminale sia il deficit di risposta, evitando di scambiare un alto numero di incidenti pubblici per debolezza istituzionale automatica.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (8,5/10) e attori incorporati nello Stato (8,0/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Yemen assumono particolare rilevanza phishing e credential theft, ransomware, frodi d'investimento, attacchi a energia e servizi pubblici, abuso di cripto-attività e campagne che possono combinare profitto, spionaggio e pressione politica. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Yemen, la resilienza complessiva è molto debole (1,9/10); la cooperazione internazionale è molto debole (3,0/10), le politiche e norme nazionali sono molto deboli (2,0/10) e la capacità delle forze dell'ordine è molto debole (2,0/10). Completano il quadro antiriciclaggio 2,0/10, prevenzione 1,5/10 e supporto a vittime e testimoni 1,5/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Yemen, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Yemen. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Yemen, In Yemen le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. La superficie di

rischio comprende frodi, sostituzione fraudolenta della SIM, data broker, applicazioni con permessi eccessivi e assistenza remota non trasparente.

Tecnologie governative e servizi pubblici. Per Yemen, Il livello governativo di Yemen presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Yemen, Sul piano militare e dual-use, Yemen mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Yemen, Quadro normativo in evoluzione o frammentato tra privacy, telecomunicazioni, sicurezza nazionale e piattaforme. La concreta applicazione e i poteri pubblici richiedono assistenza legale locale e misure tecniche supplementari. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Yemen, Assenza di adeguatezza UE e capacità di rimedio non sempre verificabile. Eventuali flussi richiedono SCC, TIA, cifratura con chiavi sotto controllo italiano, minimizzazione e un piano di rientro/continuità; per categorie strategiche la scelta prudente è il trattamento in Italia o nel SEE. La componente FOTR di trasferibilità è 3,7/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
2,3	1,2	2,4	3,6	1,3	2,2

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
5,2	4,8	4,0	5,0	4,2	3,7

Il GCRI di Yemen è 2,2/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è positivo: allineamento normativo, cooperazione e garanzie istituzionali rendono il rapporto più affidabile di quanto suggeriscano alcuni limiti tecnici. Tra le componenti FOTR, il valore più alto è Compatibilità giuridica (5,2/10), mentre il più basso è Trasferibilità dati (3,7/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Yemen, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Yemen, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Yemen, Dal punto di vista italiano, Yemen rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Yemen ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

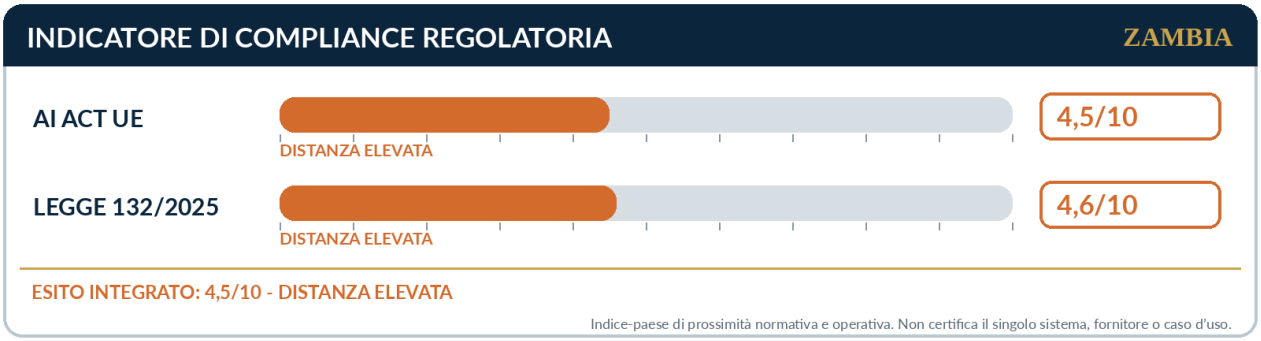
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Yemen: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 6/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Zambia

Posizione FOTR	159	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	4,5	GCRI / 10	5,1	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Zambia, AI Act UE 4,5/10; legge 132/2025 4,6/10; esito integrato 4,5/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Il profilo tecnologico di Zambia, situato in Africa orientale, deve essere letto insieme al suo assetto istituzionale e alle dipendenze esterne. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è parzialmente libero con 53/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (5,1/10) e indice FOTR (4,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per Zambia non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	17,1% / 0,8 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	53,6% / 81 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	54,2 / 60,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	92,6/100 - Tier 2 - avanzato	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	47,3/100 - rank 82	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	62/100 - Parzialmente libero / Parzialmente libero (53/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,0 / 4,7 / 5,3	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Zambia, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Zambia le evidenze principali sono GTMI 60,2/100, EGDI 54,2/100, GCI 92,6/100, AI readiness 47,3/100. La dimensione più robusta è postura di sicurezza cyber (7,2/10), mentre la criticità relativa riguarda maturità infrastrutturale (3,3/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Zambia è 3,3/10. La base statistica rileva utenti Internet pari al 17,1% nel 2024; 0,8 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 53,6% nel 2024; 81 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Zambia al posto 82 con un valore medio di 47,3/100; il pilastro migliore è governance (61,2/100), quello più debole è sviluppo e diffusione (30,1/100). Il GTMI 2025 è 60,2/100. Il punteggio S2 è 4,9/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Zambia è valutata sufficiente ma disomogenea, con S3 pari a 5,2/10. Le evidenze disponibili comprendono indice UN di capitale umano 62,3/100, sviluppo e diffusione dell'IA 30,1/100, penetrazione Internet 17,1%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Zambia ottiene S4 4,8/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Zambia, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre ricavabile dalla

sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,8/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Zambia è S5 7,2/10. La base ITU registra ITU GCI 92,6/100, Tier 2 - avanzato; il pilastro relativamente più debole è sviluppo delle capacità (15,0/20). Freedom on the Net è 62/100 - Parzialmente libero, mentre Freedom in the World è Parzialmente libero (53/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,0	Crimini finanziari	5,5
Reti criminali	6,0	Attori incorporati nello Stato	6,5
Attori stranieri	7,0	Attori del settore privato	3,5
Resilienza complessiva	4,7	Cooperazione internazionale	5,5
Politiche e norme nazionali	6,5	Forze dell'ordine	4,0
Antiriciclaggio	5,5	Prevenzione	4,0
Supporto vittime e testimoni	3,0	Rischio operativo FOTR-CY	5,3 - SIGNIFICATIVO

Esposizione cybercriminale. La combinazione fra reati cyber-dipendenti (4,0/10), criminalità finanziaria (5,5/10) e resilienza (4,7/10) colloca Zambia in una fascia di rischio significativo, pari a 5,3/10. Una bassa incidenza osservata non equivale automaticamente a sicurezza: può riflettere minore digitalizzazione, sottodenuncia o capacità forense insufficiente.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori stranieri (7,0/10) e attori incorporati nello Stato (6,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Zambia assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Zambia, la resilienza complessiva è debole (4,7/10); la cooperazione internazionale è intermedia (5,5/10), le politiche e norme nazionali sono intermedie (6,5/10) e la capacità delle forze dell'ordine è debole (4,0/10). Completano il quadro antiriciclaggio 5,5/10, prevenzione 4,0/10 e supporto a vittime e testimoni 3,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Zambia, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money; verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Zambia. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Zambia, In Zambia le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i partner

italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Zambia, Il livello governativo di Zambia presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Zambia, Sul piano militare e dual-use, Zambia mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Zambia, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Zambia, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,4/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,3	4,9	5,2	4,8	7,2	5,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,7	4,2	4,4	5,1	4,0	4,4

Il GCRI di Zambia è 5,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è negativo: capacità tecnica e dimensione di mercato non compensano pienamente le criticità di diritto, strategia, controllo pubblico o trasferimento dei dati. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,1/10), mentre il più basso è Supply chain (4,0/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Zambia, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Zambia, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Zambia, Dal punto di vista italiano, Zambia rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Zambia ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

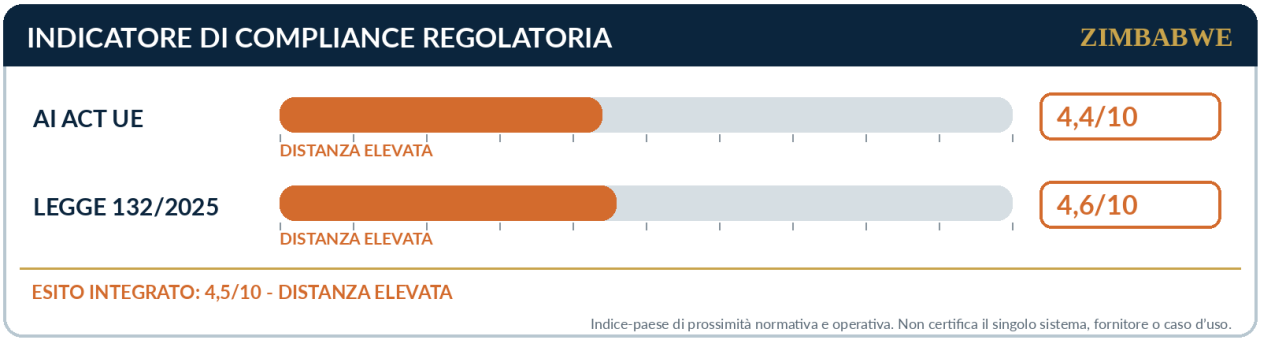
Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Zambia: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Zimbabwe

Posizione FOTR	160	Area	Africa	Subregione	Africa orientale
Status	Stato membro delle Nazioni Unite	Confidenza Celeborn Intelligence	Alta	Copertura dati	7/7 famiglie
FOTR / 10	4,5	GCRI / 10	4,1	Classe operativa	Rischio alto

Compliance con AI Act e legge 132/2025



Lettura operativa. Nel caso di Zimbabwe, AI Act UE 4,4/10; legge 132/2025 4,6/10; esito integrato 4,5/10, classe «Distanza elevata». Il punteggio esprime quanto l'ecosistema nazionale renda prevedibile l'adempimento di un operatore italiano; non presuppone che la normativa europea sia recepita localmente. L'AI Act può comunque rilevare quando sistemi o output raggiungono il mercato dell'Unione. La distanza è elevata: limitare i casi d'uso, escludere dati critici, imporre controllo tecnico dal SEE e subordinare il rapporto a verifica legale e cyber indipendente.

Premessa geopolitica e tecnologica

Per un operatore italiano, Zimbabwe non è soltanto un mercato digitale: è un insieme di vincoli territoriali, normativi e strategici. La crescita dei servizi mobili e fintech convive spesso con capacità amministrative, energetiche e di sicurezza disomogenee; infrastrutture e rimedi devono quindi essere verificati a livello di singolo progetto. Il territorio è classificato come senza sbocco al mare; tale caratteristica influenza ridondanza dei collegamenti e capacità di ripristino. La provenienza prevalente stimata della tecnologia è: Italia/UE, Stati Uniti, Cina, India. Il quadro di libertà e controlli istituzionali, misurato da Freedom in the World 2026, è non libero con 25/100. Questo dato non misura la cybersicurezza, ma contribuisce a valutare trasparenza, rimedi e prevedibilità degli accessi pubblici. GCRI tecnico (4,1/10) e indice FOTR (4,5/10) risultano vicini, segnalando coerenza tra capacità tecnologica e affidabilità operativa verso l'Italia.

Esito sintetico

Quadro sintetico. Per Zimbabwe non è prudente assumere equivalenza con gli standard italiani o UE. Ogni progetto richiede verifica della controparte, minimizzazione dei dati e un piano di continuità fuori dalla giurisdizione.

Indicatori Celeborn Intelligence comparabili

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Connettività	Utenti Internet / banda fissa	41,6% / 1,9 per 100	2024/2024	S1: accesso e maturità delle reti
Continuità	Elettricità / server sicuri	62,0% / 90 per milione	2024/2024	S1 e S5: continuità e superficie digitale
Governo digitale	UN EGDI / World Bank GTMI	44,8 / 45,2	2024 / 2025	S2-S3: servizi pubblici, sistemi e abilitatori
Cybersecurity	ITU GCI e tier	39,9/100 - Tier 4 - in evoluzione	2024	S5: misure legali, tecniche, organizzative, capacità e cooperazione
Intelligenza artificiale	Government AI Readiness	29,4/100 - rank 126	2025	S2-S3: capacità pubblica, infrastrutture, governance e resilienza

Dimensione	Indicatore	Valore	Anno	Uso nella valutazione
Libertà digitale	Freedom on the Net / Freedom in the World	50/100 - Parzialmente libero / Non libero (25/100)	2025 / 2026	S3-S5 e FOTR: diritti, trasparenza, censura e rimedi
Dati e cooperazione	Adeguatezza UE / Convenzione di Budapest	Nessuna decisione generale di adeguatezza UE / Non parte o status non comparabile	agg. 2026	FOTR: trasferibilità dati e cooperazione su evidenza elettronica
Cybercrime organizzato	GI-TOC reati cyber-dipendenti / resilienza / FOTR-CY	4,5 / 3,0 / 6,3	2025	S5 e decisione: prevalenza criminale, risposta e presidi

Nel profilo di Zimbabwe, n.d. indica un dato non disponibile o non attribuibile con sufficiente comparabilità. La copertura è 7/7 famiglie; i valori arrotondati servono al confronto e non sostituiscono la fonte originale.

Interpretazione degli indicatori. La tabella non è un riepilogo ornamentale: costituisce la base quantitativa usata per costruire i cinque punteggi tecnici. Per Zimbabwe le evidenze principali sono GTMI 45,2/100, EGDI 44,8/100, GCI 39,9/100, AI readiness 29,4/100. La dimensione più robusta è capitale umano e competenze digitali (4,5/10), mentre la criticità relativa riguarda adozione di IA e tecnologie emergenti (3,4/10). Sono disponibili 7 famiglie di dati comparabili e la confidenza Celeborn Intelligence è classificata alta. Un valore mancante non viene trasformato automaticamente in zero: riduce la confidenza, attiva richieste di verifica e limita l'uso del punteggio per decisioni irreversibili.

Infrastrutture, telecomunicazioni e resilienza

Il punteggio S1 di Zimbabwe è 3,6/10. La base statistica rileva utenti Internet pari al 41,6% nel 2024; 1,9 abbonamenti fissi ogni 100 abitanti nel 2024; accesso all'elettricità del 62,0% nel 2024; 90 server Internet sicuri per milione di abitanti nel 2024. Il quadro sintetico delle reti è descritto come maturità infrastrutturale limitata, con dipendenze fisiche e operative che possono compromettere continuità e controllo. L'assenza di accesso diretto al mare aumenta la dipendenza da dorsali terrestri e da Paesi di transito; la resilienza va verificata attraverso rotte fisicamente separate, accordi con carrier diversi e continuità elettrica delle stazioni di frontiera. I valori di accesso all'elettricità non misurano da soli ridondanza, qualità della rete o disponibilità di gruppi di continuità. Analogamente, la diffusione del 5G non dimostra che il core sia standalone, che gli apparati siano sostituibili o che la copertura riguardi aree industriali e governative. Prima di investire occorre quindi acquisire mappe di rete, fornitori RAN/core, SLA, localizzazione dei data center e piani di disaster recovery.

Intelligenza artificiale e tecnologie emergenti

Oxford Insights colloca Zimbabwe al posto 126 con un valore medio di 29,4/100; il pilastro migliore è governance (53,0/100), quello più debole è politiche pubbliche (12,0/100). Il GTMI 2025 è 45,2/100. Il punteggio S2 è 3,4/10 e indica una capacità limitata. L'indice considera policy, cloud, servizi pubblici, ecosistema di sviluppo e infrastrutture di calcolo, ma non presume l'esistenza di capacità HPC sovrana, modelli linguistici nazionali o data center controllati dallo Stato in assenza di evidenze. IoT, smart city, robotica, sistemi autonomi e quantum devono essere analizzati per progetto: vanno identificati dataset di addestramento, Paese di esecuzione, dipendenze API, origine degli acceleratori, accesso amministrativo, aggiornamenti e possibilità di esportare modelli e log. Per la crittografia post-quantum è necessario verificare roadmap concrete, non semplici programmi di ricerca.

Capitale umano, formazione e competenze STEM

La dotazione di capitale umano di Zimbabwe è valutata fragile, con S3 pari a 4,5/10. Le evidenze disponibili comprendono indice UN di capitale umano 53,9/100, sviluppo e diffusione dell'IA 23,0/100, penetrazione Internet 41,6%. Il numero di laureati STEM, la qualità dei percorsi di ingegneria, la disponibilità di professionisti cyber e il saldo tra attrazione e fuga dei talenti non sono uniformemente misurabili per tutte le 208 entità; per questo non vengono inventati valori mancanti. Nella verifica preventiva operativa si devono acquisire dati aggiornati su università, certificazioni, lingua di lavoro, turnover, dipendenza da consulenti esteri e possibilità di trattenere personale qualificato. Una popolazione molto connessa non equivale a competenze avanzate, mentre un piccolo ecosistema specialistico può sostenere progetti d'eccellenza senza garantire capacità diffusa nella pubblica amministrazione.

Supply chain, fornitori e sovranità tecnologica

La supply chain di Zimbabwe ottiene S4 4,4/10 e presenta forte dipendenza esterna o concentrazione. La provenienza prevalente stimata è Italia/UE, Stati Uniti, Cina, India; l'indicatore di indipendenza disponibile è 5,0/10. La voce aggrega hardware di rete, semiconduttori, sistemi operativi, software applicativo, cloud, servizi di sicurezza e manutenzione. Non si attribuisce capacità produttiva domestica di semiconduttori o componenti critici senza evidenze verificabili: un assemblaggio locale può dipendere interamente da progettazione, firmware, macchinari o licenze straniere. Per i contratti italiani devono essere mappati produttore effettivo, distributore, centro assistenza, Paesi di supporto, telemetria, repository, chiavi di firma, componenti open source e subfornitori. L'uso di più marchi non costituisce diversificazione se il controllo ultimo appartiene allo stesso gruppo o se tutti dipendono dal medesimo hyperscaler.

Fornitore o ecosistema prevalente. Nel caso di Zimbabwe, Presenza frequente di fornitori cinesi nelle reti e nelle infrastrutture, affiancata da operatori europei, statunitensi, indiani, turchi, del Golfo e locali. L'origine effettiva non è sempre

ricavabile dalla sola controparte contrattuale. L'impatto sulla valutazione è misurato da S4=4,4/10 e dal proxy di indipendenza 5,0/10; la verifica contrattuale deve risalire al controllo effettivo, non fermarsi al rivenditore.

Cybersecurity, libertà digitale e cooperazione

La postura cyber di Zimbabwe è S5 4,4/10. La base ITU registra ITU GCI 39,9/100, Tier 4 - in evoluzione; il pilastro relativamente più debole è misure tecniche (1,4/20). Freedom on the Net è 50/100 - Parzialmente libero, mentre Freedom in the World è Non libero (25/100). Questi indicatori sono utilizzati per distinguere capacità difensiva, libertà digitale e trasparenza: un Paese può avere strutture cyber potenti e al tempo stesso esercitare censura o accessi pubblici invasivi. Stato Convenzione di Budapest: Non parte o status non comparabile. Quadro normativo sintetico: Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate.. L'Atlante non assegna un bonus o una penalità automatica in base al numero di incidenti resi pubblici, perché i Paesi più trasparenti riportano più eventi. Lo storico degli attacchi, l'operatività del CERT/CSIRT, i tempi di notifica e le interruzioni arbitrarie della rete devono essere aggiornati annualmente e verificati prima dell'avvio di servizi essenziali.

Cybercrime: minacce, capacità di contrasto e rischio per l'Italia

Chiave di lettura. Nei mercati criminali un valore alto è sfavorevole; nella resilienza e nei presidi istituzionali un valore alto è favorevole. La tabella distingue pertanto pressione criminale e capacità di risposta.

Indicatore	Valore / 10	Indicatore	Valore / 10
Reati cyber-dipendenti	4,5	Crimini finanziari	6,5
Reti criminali	7,5	Attori incorporati nello Stato	8,0
Attori stranieri	6,5	Attori del settore privato	5,0
Resilienza complessiva	3,0	Cooperazione internazionale	3,5
Politiche e norme nazionali	3,5	Forze dell'ordine	2,5
Antiriciclaggio	4,0	Prevenzione	4,0
Supporto vittime e testimoni	2,0	Rischio operativo FOTR-CY	6,3 - SIGNIFICATIVO

Rischio criminale connesso alle tecnologie. In Zimbabwe il rapporto tra opportunità digitali e capacità criminali produce un indicatore di 6,3/10, livello significativo. I reati che dipendono direttamente da sistemi informatici raggiungono 4,5/10; le frodi e i reati finanziari 6,5/10. La lettura operativa considera anche la qualità della risposta pubblica e la possibilità concreta di acquisire, conservare e scambiare prova digitale.

Attori, infrastrutture e vettori prioritari. Il profilo degli attori è guidato da attori incorporati nello Stato (8,0/10) e reti criminali (7,5/10). Questa combinazione orienta la verifica preventiva verso proprietà effettiva, subfornitura, accessi privilegiati, intermediari finanziari e possibili connessioni istituzionali o transnazionali. Nella valutazione preliminare del profilo di Zimbabwe assumono particolare rilevanza frodi sui servizi di denaro mobile, sostituzione fraudolenta della SIM, compromissione delle caselle di posta aziendale, phishing, frodi su identità e prestiti digitali, truffe in cripto-attività e sfruttamento di capacità investigative o di reporting non uniformi. La presenza di un vettore nel profilo non implica che ogni operatore locale sia compromesso; indica le verifiche da rendere obbligatorie prima di collegare sistemi, delegare assistenza o trasferire credenziali e dati.

Capacità di contrasto e cooperazione probatoria. Nel caso di Zimbabwe, la resilienza complessiva è molto debole (3,0/10); la cooperazione internazionale è debole (3,5/10), le politiche e norme nazionali sono deboli (3,5/10) e la capacità delle forze dell'ordine è molto debole (2,5/10). Completano il quadro antiriciclaggio 4,0/10, prevenzione 4,0/10 e supporto a vittime e testimoni 2,0/10. Per l'Italia questi dati incidono sui tempi attesi di risposta, sulla validità della catena di custodia, sulla possibilità di congelare proventi e sulla prevedibilità dell'assistenza giudiziaria o amministrativa.

Implicazioni per soggetti italiani. Nei rapporti con soggetti operanti in Zimbabwe, il livello significativo non determina da solo un divieto, ma modifica il perimetro accettabile: verifica indipendente della proprietà e dei subfornitori; autenticazione multifattore (MFA) resistente al phishing e separazione delle utenze amministrative; registri immutabili con conservazione in Italia o nel SEE; clausole di notifica immediata, cooperazione forense e preservazione della prova; segmentazione a fiducia zero e divieto di fiducia implicita tra domini; copie di sicurezza offline testate e piano di risposta a ransomware ed estorsione mediante sottrazione o cifratura dei dati; monitoraggio continuo di credenziali esposte, domini, portafogli digitali e infrastrutture malevole; procedure anti-SIM-swap, verifica fuori banda dei pagamenti e presidio delle frodi mobile-money.

Fonte cybercrime: Global Organized Crime Index 2025 (GI-TOC), valori 0-10; dato nazionale GI-TOC 2025 riferito al profilo di Zimbabwe. L'indice FOTR-CY è un'elaborazione prudenziale della Fondazione e non una statistica giudiziaria nazionale.

Tecnologie civili, governative e dual-use

Tecnologie per popolazione e imprese. Per Zimbabwe, In Zimbabwe le tecnologie destinate alla popolazione mostrano adozione digitale significativa ma disomogenea, spesso concentrata nelle aree urbane e dipendente da pochi operatori. Per i

partner italiani occorre valutare profilazione commerciale, identità, localizzazione dei dispositivi e possibilità di trasferimento verso Paesi terzi.

Tecnologie governative e servizi pubblici. Per Zimbabwe, Il livello governativo di Zimbabwe presenta digitalizzazione pubblica disomogenea, appalti concentrati e dipendenza da operatori esterni o da infrastrutture centralizzate. I progetti con il settore pubblico richiedono audit sulla segregazione degli ambienti, gestione delle identità privilegiate e conservazione delle evidenze.

Tecnologie militari e dual-use. Per Zimbabwe, Sul piano militare e dual-use, Zimbabwe mostra capacità pubblicamente documentabili limitate o frammentate e dipendenza da fornitori esteri. L'Atlante non valuta vulnerabilità operative: per l'Italia rilevano controllo delle esportazioni, sanzioni, utilizzatore finale e destinazione d'uso, proprietà intellettuale, accesso al codice e rischio di riutilizzo non autorizzato.

Norme nazionali e trasferimento dei dati dall'Italia

Quadro normativo nazionale. Per Zimbabwe, Quadro privacy e cyber parziale o di recente formazione, con limitata capacità di vigilanza e rimedio. Per dati personali o strategici servono garanzie contrattuali, tecniche e organizzative rafforzate. Lo stato rispetto alla Convenzione di Budapest è: Non parte o status non comparabile; questo elemento incide sulla cooperazione, ma non sostituisce la verifica dell'attuazione effettiva.

Regime del trasferimento. Nei flussi dall'Italia verso Zimbabwe, Assenza di decisione UE di adeguatezza. Il trasferimento dall'Italia richiede una base del capo V GDPR, normalmente SCC o BCR, un Transfer Impact Assessment, misure supplementari e controllo dei trasferimenti ulteriori e degli accessi governativi. La componente FOTR di trasferibilità è 4,1/10 e il rischio sui dati personali è Medio-alto; tali valori determinano intensità della TIA, misure supplementari e localizzazione prudenziale.

Scorecard tecnica GCRI

S1 Infrastrutture	S2 IA e tech	S3 Capitale umano	S4 Supply chain	S5 Cybersecurity	GCRI finale
3,6	3,4	4,5	4,4	4,4	4,1

Componenti dell'indice FOTR

Compatibilità giuridica	Maturità cyber	Trasparenza istituzionale	Compatibilità strategica	Supply chain	Trasferibilità dati
4,7	4,5	4,5	5,2	4,1	4,1

Il GCRI di Zimbabwe è 4,1/10 e deriva dalla media aritmetica di S1-S5, ciascuno con peso del 20%. L'indice FOTR finale è 4,5/10 e rappresenta la decisione operativa dal punto di vista italiano. Il correttivo italiano è contenuto: la valutazione tecnica e quella istituzionale convergono senza scostamenti rilevanti. Tra le componenti FOTR, il valore più alto è Compatibilità strategica (5,2/10), mentre il più basso è Supply chain (4,1/10). Le tabelle devono essere lette congiuntamente: il GCRI descrive la maturità del Paese; il FOTR stabilisce quanto quella maturità sia utilizzabile da un soggetto italiano senza trasferire rischi non accettabili.

Matrice dei rischi per settore

Dati personali	Sanità e biometria	Cloud e infrastrutture	IP e R&S	Pubblica amministrazione	Difesa e dual-use
Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto	Medio-alto

La matrice applica il FOTR di 4,5/10 alle sei categorie operative, evitando di trasferire automaticamente al singolo contratto la reputazione generale del Paese. Per Zimbabwe, 6 ambiti richiedono autorizzazione rafforzata o possibile esclusione: Dati personali, Sanità e biometria, Cloud e infrastrutture, IP e R&S, Pubblica amministrazione, Difesa e dual-use. La conseguenza pratica è graduare minimizzazione, segregazione, autorizzazioni, audit indipendente ed exit plan in funzione del dato e dell'asset coinvolto. Nel rapporto con Zimbabwe, sanità, biometria, pubblica amministrazione, difesa e proprietà intellettuale devono quindi essere trattate come decisioni autonome, anche quando il rischio complessivo appare contenuto.

Valutazione e presidi per operatori italiani

Valutazione centrata sull'Italia. Nel rapporto tra Italia e Zimbabwe, Dal punto di vista italiano, Zimbabwe rientra nella classe «Criticità controllata»: cooperazione circoscritta a perimetri non critici, subordinata a architettura isolata, dati minimizzati o pseudonimizzati, supervisione italiana e diritto di recesso immediato. Il punteggio non sostituisce golden power, controllo export, procurement pubblico, antiriciclaggio o valutazioni di sicurezza nazionale.

Decisione operativa indicativa. Il rapporto con Zimbabwe ricade nella fascia di alto rischio (4,5/10): utilizzare ambienti segregati e dati minimizzati, applicare garanzie rafforzate ed escludere funzioni strategiche, con particolare attenzione a Dati personali.

Presidi minimi raccomandati

Evitare dati sanitari, biometrici, giudiziari, di difesa o relativi a infrastrutture critiche.

Usare architetture isolate, dati pseudonimizzati e chiavi non disponibili alla controparte locale.

Prevedere supervisione continua, kill switch contrattuale e rientro immediato dei dati.

Verificare proprietà, influenza statale, sanzioni, utilizzatore finale e destinazione d'uso e validità dei rimedi.

Profilo Celeborn Intelligence di Zimbabwe: World Development Indicators, valori più recenti disponibili 2022-2024; UN DESA E-Government Survey 2024; ITU Global Cybersecurity Index 2024; World Bank GovTech Maturity Index 2025; Oxford Insights Government AI Readiness Index 2025; Freedom House, Freedom on the Net 2025; Freedom House, Freedom in the World 2026; Commissione europea, regime dei trasferimenti di dati aggiornato alla chiusura editoriale; Consiglio d'Europa, stato della Convenzione di Budapest. Confidenza complessiva Alta con copertura 7/7 famiglie. Chiusura informativa dell'Atlante: 5 agosto 2026.

Matrice decisionale per istituzioni e operatori italiani

FOTR	Postura	Dati personali	Cloud/PA	IP e R&S	Difesa/dual-use
8,0-10,0	Cooperazione ordinaria controllata	Ammissibili con GDPR	Ammissibili con qualifica e audit	Ammissibili con tutela IP	Ammissibili previa disciplina export/utilizzatore finale e destinazione d'uso
6,5-7,9	Cooperazione condizionata	SCC/TIA se necessario	Segregazione e exit plan	Limitare accesso a know-how critico	Autorizzazione e controllo rafforzato
5,0-6,4	Cooperazione selettiva	Minimizzazione e cifratura	No lock-in; chiavi in Italia/SEE	Sandbox e compartimentazione	Evitare capacità sensibili salvo autorizzazione
3,5-4,9	Alto rischio	Evitare categorie speciali salvo necessità	Niente servizi essenziali senza segregazione	Niente codice/dataset critici	Presunzione di esclusione
0,0-3,4	Rischio estremo	Non trasferire salvo eccezione autorizzata	Nessun accesso a reti interne	Nessun know-how strategico	Non cooperazione salvo finalità autorizzate

La matrice è una soglia minima. Settori regolati, informazioni classificate, infrastrutture critiche e dati sanitari possono richiedere condizioni più severe indipendentemente dal punteggio nazionale.

Checklist pre-ingaggio

Area	Domande obbligatorie	Esito
Identità e controllo	Titolare effettivo, gruppo societario, partecipazioni pubbliche, sanzioni, reputazione, conflitti di interesse.	◻ Conforme ◻ Da integrare ◻ Non ammissibile
Dati	Categorie, finalità, minimizzazione, localizzazione, accessi remoti, subresponsabili, trasferimenti ulteriori, cancellazione.	◻ Conforme ◻ Da integrare ◻ Non ammissibile
Architettura	Reti, cloud, API, dipendenze, RAN/core, data center, backup, chiavi, logging, autenticazione privilegiata.	◻ Conforme ◻ Da integrare ◻ Non ammissibile
Supply chain	Produttore, firmware, SBOM, componenti, repository, firma degli aggiornamenti, supporto, parti di ricambio.	◻ Conforme ◻ Da integrare ◻ Non ammissibile
Cybersecurity	CERT/CSIRT, incident response, notifica, penetration test, vulnerability management, business continuity.	◻ Conforme ◻ Da integrare ◻ Non ammissibile
IA e algoritmi	Modello, addestramento, dataset, bias, spiegabilità, supervisione umana, output, sicurezza, dipendenze esterne.	◻ Conforme ◻ Da integrare ◻ Non ammissibile
Proprietà intellettuale	Titolarità, licenze, riuso, accesso al codice, brevetti, segreti industriali, dataset di addestramento.	◻ Conforme ◻ Da integrare ◻ Non ammissibile
Diritto e contratti	Legge applicabile, foro, SCC/BCR, TIA, audit, ispezioni, responsabilità, assicurazione, subfornitura.	◻ Conforme ◻ Da integrare ◻ Non ammissibile
Exit strategy	Portabilità, formati, cancellazione verificabile, migrazione, sostituzione, escrow, disattivazione sicura.	◻ Conforme ◻ Da integrare ◻ Non ammissibile
Sicurezza nazionale	Golden power, procurement, export control, dual-use, classificazione, autorizzazioni e pareri competenti.	◻ Conforme ◻ Da integrare ◻ Non ammissibile

Protocollo di aggiornamento annuale

L'Atlante deve essere aggiornato almeno una volta l'anno e ogni volta che si verifica un evento capace di alterare in modo materiale l'affidabilità digitale. La revisione non consiste nel cambiare soltanto i punteggi: richiede la conservazione delle fonti, la motivazione delle variazioni e un controllo di coerenza tra dati quantitativi e giudizio italiano.

Aggiornare dataset globali e registrare anno, versione, copertura e modifiche metodologiche.
Verificare nuove leggi nazionali su dati, cyber, IA, cloud, telecomunicazioni, sorveglianza e sicurezza nazionale.
Mappare accordi tecnologici, investimenti esteri, cambi di fornitori, cavi, data center, satelliti e infrastrutture energetiche.
Raccogliere incidenti significativi, shutdown, sanzioni, conflitti, colpi di Stato e cambi di riconoscimento internazionale.
Ricalcolare S1-S5 e documentare separatamente il correttivo FOTR centrato sull'Italia.
Sottoporre i profili con variazione superiore a 0,5 punti o classe di rischio diversa a revisione umana rafforzata.
Conservare una versione storica per consentire audit, confronto e ricostruzione delle decisioni istituzionali.

Glossario essenziale

Termine	Definizione
Adeguatezza UE	Decisione della Commissione europea che riconosce un livello di protezione dei dati sostanzialmente equivalente, consentendo flussi assimilati a quelli intra-SEE.
BCR	Binding Corporate Rules per trasferimenti infragruppo di dati personali.
CERT/CSIRT	Struttura per prevenzione, gestione e coordinamento degli incidenti informatici.
GCRI	Indice tecnico medio S1-S5, con peso del 20% per ciascuna dimensione.
FOTR	Indice finale di affidabilità digitale centrato sugli interessi e obblighi dell'Italia.
HPC	High Performance Computing, capacità di calcolo ad alte prestazioni.
Hyperscaler	Fornitore cloud globale con infrastruttura e servizi su scala molto ampia.
Celeborn Intelligence	Raccolta e analisi di informazioni da fonti aperte e legalmente accessibili.
PQC	Crittografia post-quantum progettata per resistere a futuri attacchi quantistici.
RAN	Radio Access Network delle reti mobili; distinta dal core di rete.
SCC	Clausole contrattuali standard della Commissione europea per trasferimenti verso Paesi terzi.
SBOM	Software Bill of Materials, inventario dei componenti software.
TIA	Transfer Impact Assessment per valutare legge e prassi del Paese terzo e misure supplementari.
Dual-use	Beni, software e tecnologie utilizzabili sia in ambito civile sia militare.
Exit plan	Piano verificabile per migrare dati e servizi, revocare accessi e sostituire il fornitore.

Bibliografia e fonti di riferimento

World Bank, GovTech Maturity Index 2025: Tracking Public Sector Digital Transformation Worldwide, dataset e metodologia su 197 economie.
World Bank, World Development Indicators: Individuals using the Internet; fixed broadband subscriptions; secure Internet servers; access to electricity.
United Nations Department of Economic and Social Affairs, E-Government Survey 2024.
International Telecommunication Union, Global Cybersecurity Index 2024 e Global Cybersecurity Knowledgebase.
Oxford Insights, Government AI Readiness Index 2025, 195 governi e sei pilastri di valutazione.
Freedom House, Freedom on the Net 2025 e relativa metodologia, 72 Paesi.
Freedom House, Freedom in the World 2026, 208 Paesi e territori; dati elaborati anche tramite Our World in Data.
Commissione europea, decisioni di adeguatezza, Standard Contractual Clauses, Binding Corporate Rules e regole sui trasferimenti internazionali.
Consiglio d'Europa, Convenzione di Budapest, protocolli, elenco delle Parti e attività T-CY.
Nazioni Unite, Convenzione contro la criminalità informatica e United Nations Treaty Collection.

Unione europea, GDPR, NIS2, CER, DORA, Cyber Resilience Act, Data Governance Act, Data Act, AI Act, DSA, DMA, eIDAS 2.0 e atti collegati.

Repubblica italiana, Codice privacy, CAD, d.lgs. 138/2024, legge 90/2024, perimetro di sicurezza nazionale cibernetica, disciplina ACN, golden power, legge 132/2025 e norme settoriali.

BYD, Accordo tra BYD e la Repubblica di San Marino: al via la sperimentazione di tecnologie energetiche integrate, 24 marzo 2026.

Segreterie di Stato della Repubblica di San Marino / San Marino RTV, missione strategica a Shenzhen tra tecnologia e sostenibilità, 15 maggio 2026.

Le fonti sono state consultate in italiano, inglese e, quando necessario, in altre lingue. Nel volume le informazioni sono uniformate e presentate esclusivamente in italiano.

Unione europea, regolamento (UE) 2024/1689 (Artificial Intelligence Act), testo consolidato al 27 luglio 2026, e regolamento (UE) 2026/1744 (Digital Omnibus on AI).

Repubblica italiana, legge 23 settembre 2025, n. 132, Disposizioni e deleghe al Governo in materia di intelligenza artificiale, con avviso di rettifica del 17 ottobre 2025.

Global Initiative Against Transnational Organized Crime, Global Organized Crime Index 2025: dataset aperto, metodologia, scoring thresholds e guiding questions.

Europol, valutazioni strategiche sulla criminalità organizzata e sulle minacce cyber; INTERPOL, assessment regionali e strumenti per cooperazione e prova digitale.

Destinatari istituzionali e finalità strategica

Origine e finalità della ricerca

L'Atlante dell'affidabilità digitale è una ricerca autonoma ideata, promossa e realizzata dalla Fondazione Olivetti Tecnologia e Ricerca. Nasce dall'esigenza di trasformare fonti pubbliche, indicatori internazionali e analisi geopolitiche in uno strumento coerente con le responsabilità, le norme e gli interessi strategici dell'Italia.

La Fondazione ha sviluppato il volume per offrire un contributo fattivo allo sviluppo e alla protezione del Paese e delle sue principali istituzioni. L'obiettivo è sostenere la qualità delle decisioni relative agli investimenti digitali, alla cooperazione internazionale, all'acquisizione di tecnologie, al trasferimento dei dati, alla difesa delle infrastrutture critiche, alla sicurezza della ricerca e alla continuità dei servizi pubblici.

Il documento è concepito come supporto strategico preliminare, verificabile e aggiornabile. Non sostituisce l'intelligence classificata, i pareri legali, le verifiche sanzionatorie, le valutazioni di sicurezza nazionale, gli audit tecnici o le istruttorie amministrative; consente tuttavia di individuare in anticipo le aree nelle quali tali approfondimenti devono essere attivati, coordinati e documentati.

L'impiego del metodo Celeborn Intelligence permette di ricondurre evidenze eterogenee a criteri comparabili e a raccomandazioni orientate all'Italia. La ricerca intende favorire una cultura istituzionale della prevenzione, della sovranità tecnologica, della responsabilità nella condivisione dei dati e della cooperazione internazionale consapevole.

Destinatari prioritari

Il volume è destinato, in via prioritaria e senza pretesa di esaustività, alle istituzioni e agli organismi pubblici chiamati a tutelare la continuità dello Stato, la sicurezza nazionale, i diritti fondamentali, l'economia, la ricerca, le infrastrutture e la proiezione internazionale dell'Italia.

Organi costituzionali e indirizzo politico-strategico

- Presidenza della Repubblica.
- Presidenza del Consiglio dei ministri e Dipartimenti della Presidenza competenti per trasformazione digitale, funzione pubblica, politiche europee, programmazione economica e coordinamento delle emergenze.
- Camera dei deputati.
- Senato della Repubblica.
- Comitato parlamentare per la sicurezza della Repubblica (COPASIR).
- Commissioni parlamentari competenti in materia di affari costituzionali, esteri, difesa, bilancio, attività produttive, telecomunicazioni, trasporti, ambiente, salute, ricerca e politiche dell'Unione europea.

Sicurezza nazionale, intelligence e cybersicurezza

- Comitato interministeriale per la sicurezza della Repubblica (CISR).
- Dipartimento delle informazioni per la sicurezza (DIS).
- Agenzia informazioni e sicurezza esterna (AISE).
- Agenzia informazioni e sicurezza interna (AISI).
- Agenzia per la cybersicurezza nazionale (ACN).
- CSIRT Italia.
- Comitato interministeriale per la cybersicurezza (CIC).
- Dipartimento della Protezione Civile.

Amministrazioni centrali dello Stato

- Ministero degli Affari Esteri e della Cooperazione Internazionale.
- Ministero dell'Interno.
- Ministero della Giustizia.
- Ministero della Difesa.
- Ministero dell'Economia e delle Finanze.
- Ministero delle Imprese e del Made in Italy.
- Ministero dell'Agricoltura, della Sovranità Alimentare e delle Foreste.
- Ministero dell'Ambiente e della Sicurezza Energetica.
- Ministero delle Infrastrutture e dei Trasporti.
- Ministero del Lavoro e delle Politiche Sociali.
- Ministero dell'Istruzione e del Merito.
- Ministero dell'Università e della Ricerca.
- Ministero della Cultura.

- Ministero della Salute.
- Ministero del Turismo.

Difesa, sicurezza pubblica, giustizia e contrasto al cybercrime

- Stato Maggiore della Difesa.
- Esercito Italiano, Marina Militare e Aeronautica Militare.
- Arma dei Carabinieri.
- Guardia di Finanza.
- Polizia di Stato, con particolare riferimento alla Polizia Postale e per la Sicurezza Cibernetica.
- Corpo nazionale dei Vigili del fuoco.
- Direzione nazionale antimafia e antiterrorismo.
- Dipartimento dell'Amministrazione Penitenziaria e articolazioni giudiziarie competenti per criminalità informatica, terrorismo, sicurezza economica e prova digitale.

Autorità indipendenti, regolazione, dati e vigilanza finanziaria

- Garante per la protezione dei dati personali.
- Agenzia per l'Italia Digitale (AgID).
- Autorità Nazionale Anticorruzione (ANAC).
- Autorità per le Garanzie nelle Comunicazioni (AGCOM).
- Autorità Garante della Concorrenza e del Mercato (AGCM).
- Banca d'Italia.
- Commissione Nazionale per le Società e la Borsa (CONSOB).
- Istituto per la Vigilanza sulle Assicurazioni (IVASS).
- Unità di Informazione Finanziaria per l'Italia (UIF).
- Autorità di Regolazione per Energia Reti e Ambiente (ARERA).
- Autorità di regolazione dei trasporti (ART).
- Corte dei conti e Istituto nazionale di statistica (ISTAT), per i profili di controllo, misurazione e valutazione delle politiche pubbliche.

Ricerca, università, salute, spazio e innovazione

- Consiglio Nazionale delle Ricerche (CNR).
- Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile (ENEA).
- Istituto Nazionale di Fisica Nucleare (INFN).
- Agenzia Spaziale Italiana (ASI).
- Istituto Superiore di Sanità (ISS).
- Agenzia Nazionale per i Servizi Sanitari Regionali (AGENAS).
- Agenzia Italiana del Farmaco (AIFA).
- Università pubbliche, Conferenza dei Rettori delle Università Italiane (CRUI), enti pubblici di ricerca e infrastrutture nazionali di calcolo e dati.
- Servizio sanitario nazionale, aziende sanitarie, aziende ospedaliere e IRCCS pubblici, con particolare riferimento ai dati sanitari, biometrici e genomici.

Territorio, rappresentanza internazionale e infrastrutture strategiche

- Regioni e Province autonome di Trento e Bolzano.
- Prefetture - Uffici territoriali del Governo.
- Città metropolitane, Province, Comuni e relative strutture ICT e di protezione civile.
- Rete diplomatica e consolare italiana e Rappresentanze permanenti presso Unione europea, NATO, Nazioni Unite e Consiglio d'Europa.
- Agenzia ICE, SACE, SIMEST, Cassa Depositi e Prestiti e Invitalia, per le attività di internazionalizzazione, sostegno agli investimenti e tutela degli interessi economici nazionali.
- Agenzia delle Entrate, Agenzia delle Dogane e dei Monopoli ed enti pubblici che amministrano dati fiscali, doganali, commerciali e transfrontalieri.
- Autorità di sistema portuale, enti di aviazione civile, gestori pubblici e società a controllo pubblico operanti nei settori della difesa, dello spazio, dell'energia, delle telecomunicazioni, dei trasporti, della finanza e dei servizi essenziali.

Criterio di destinazione e responsabilità d'uso

L'inserimento di un'istituzione nell'elenco non implica che il volume sia stato commissionato, approvato, patrocinato o formalmente acquisito da essa. La lista individua i destinatari ai quali la Fondazione ritiene utile rivolgere il documento come contributo di studio, prevenzione e supporto alla decisione, nel rispetto delle attribuzioni e delle responsabilità proprie di ciascun organismo.

La Fondazione auspica che le evidenze dell'Atlante siano sottoposte a verifica nelle sedi competenti e integrate con dati classificati, controlli tecnici, pareri giuridici e analisi settoriali. La finalità non è formulare giudizi politici assoluti sui Paesi, ma rafforzare la capacità dell'Italia di cooperare con consapevolezza, proteggere il proprio patrimonio informativo, difendere l'autonomia delle istituzioni e orientare lo sviluppo tecnologico verso condizioni di sicurezza, trasparenza e responsabilità.

Fondazione Olivetti Tecnologia e Ricerca

Massimiliano Nicolini - Capo progetto

Elenco prioritario e non esaustivo, aggiornato alla data di chiusura editoriale. L'inclusione non costituisce prova di ricezione, adesione o approvazione da parte delle istituzioni indicate.

Colophon

Titolo	Atlante dell'affidabilità digitale - Ogni nazione
Autore	Fondazione Olivetti Tecnologia e Ricerca
Capo progetto	Nicolini Massimiliano
Destinatari	Istituzioni italiane
Edizione	2026
Entità analizzate	208
Chiusura editoriale	5 agosto 2026

Fondazione Olivetti Tecnologia e Ricerca

Uso istituzionale - Celeborn Intelligence non classificato

Revisione editoriale e metodologica: indicatori AI Act/legge 132 e sezione cybercrime per 208 entità - 5 agosto 2026.