

# INDIPENDENZA DIGITALE

## 1° RAPPORTO SULL'INDIPENDENZA DIGITALE IN ITALIA

A CURA DI



**REDOPEN**

*toward a conscious present.*

PROMOSSO DA

**Key4Biz**

ORGANIZZATO DA

**SUPERCOM**  
business relations

[www.indipendenzadigitale.eu](http://www.indipendenzadigitale.eu)

## Executive Summary

Il rapporto analizza lo stato attuale e le prospettive dell'indipendenza digitale in Italia, definita come la capacità di gestire infrastrutture, dati e tecnologie critiche in modo autonomo, evitando più o meno consapevoli "rischi di dipendenza" verso soggetti terzi liberi di assumere posizioni non garantiste, opportunistiche o addirittura ostili. Viene sottolineato che "indipendenza" non significa "autarchia digitale", ma piuttosto la tutela della continuità operativa e la riduzione dei rischi derivanti da dipendenze inconsapevoli.

Il documento esamina diversi aspetti:

- **Infrastrutture digitali:** l'Italia ha compiuto progressi nel potenziare data center nazionali, reti a banda larga (la copertura è in linea con la media UE, ma per l'adozione - il take up - il nostro Paese è davvero indietro nella classifica) e reti 5G (ma per quelle stand alone siamo davvero indietro). Il Polo Strategico Nazionale (PSN), gestito da attori italiani, mira a ospitare dati e servizi critici della Pubblica Amministrazione su suolo nazionale. Nonostante la crescita di data center di grandi provider globali in Italia, permane il rischio di dipendenza nella gestione dei dati. La partecipazione a progetti europei di High-Performance Computing (HPC), come il supercomputer Leonardo, contribuisce all'indipendenza nel calcolo avanzato.
- **Software, sistemi operativi e servizi digitali:** l'Italia dipende in modo strutturale da software e piattaforme sviluppate all'estero, in particolare negli Stati Uniti. Questo comporta rischi legati alle scelte unilaterali delle aziende straniere e alle normative dei Paesi d'origine (come il Cloud Act statunitense). L'Italia e l'UE stanno reagendo con normative (come il GDPR e il Digital Services Act) e promuovendo alternative europee e l'adozione di software open source nella PA. Nonostante la crescente presenza di operatori cloud italiani ed europei, i ricavi in Europa restano largamente concentrati presso i grandi provider statunitensi.
- **Hardware e semiconduttori:** la produzione nazionale di chip avanzati e hardware è limitata, con una forte dipendenza da attori industriali non nativamente soggetti a garanzie di controllo compatibili con quelle europee. Nel settore delle telecomunicazioni, poche aziende dominano il mercato 5G, sollevando questioni di sicurezza nazionale. L'Italia ha realtà di rilievo come STMicroelectronics, che sta investendo in nuovi impianti nel paese. L'adesione all'EU Chips Act e la partecipazione a progetti IPCEI (Important Projects of Common European Interest) mirano a potenziare la filiera europea dei semiconduttori. Il livello di esposizione verso tecnologie hardware non controllabili su base nazionale o europea rimane elevato nel breve termine, ma si cercano di mitigare i rischi diversificando i fornitori e investendo in capacità nazionali/europee.
- **Dimensione Geopolitica e Rischi:** la dipendenza tecnologica da attori esterni con interessi potenzialmente divergenti costituisce un'area di vulnerabilità crescente. Paesi come Cina e Russia sono identificati come rivali geopolitici con quadri giuridici che possono obbligare le loro aziende a cooperare con i servizi di intelligence statali. La complessità delle catene di approvvigionamento globali rende difficile garantire l'integrità e la sicurezza dei componenti. I rischi associati alla dipendenza tecnologica includono spionaggio informatico, esfiltrazione di dati, sabotaggio, interruzione dei servizi, lock-in tecnologico e forme di pressione economica o politica.

- **Iniziative Italiane ed Europee:** l'Italia ha avviato diverse iniziative per rafforzare l'indipendenza digitale, sia a livello nazionale che europeo. Queste includono la strategia cloud Italia e il PSN, la partecipazione a Gaia-X per creare un ecosistema cloud federato europeo, la promozione di software open source nella PA, e la partecipazione a progetti UE su HPC, AI e competenze (EuroHPC, Programma Digital Europe, Alleanze su AI e microelettronica). L'obiettivo è costruire un sistema integrato a livello nazionale ed europeo, in grado di generare alternative tecnologiche credibili all'importazione.
- **Cybersicurezza e Protezione dei Dati:** l'Italia ha costruito un solido sistema di governance della cybersecurity con la creazione dell'Agenzia per la Cybersicurezza Nazionale (ACN) e la definizione del perimetro di sicurezza cibernetica nazionale. Nonostante i progressi, la minaccia cyber continua a crescere, in particolare con l'aumento degli attacchi ransomware e delle campagne di phishing. Le strategie nazionali puntano a rafforzare la resilienza, la formazione e lo sviluppo di tecnologie crittografiche nazionali. L'Italia beneficia del quadro normativo europeo per la tutela dei dati personali (GDPR), che ha permesso di sanzionare aziende globali per violazioni. Altre normative come il Regolamento per le infrastrutture digitali e per i servizi cloud per la PA e il futuro Data Act europeo contribuiscono alla tutela dei dati.
- **Legislazione Rilevante:** il quadro normativo italiano ed europeo è cruciale per l'indipendenza digitale. Vengono citate normative chiave come il GDPR, le Direttive NIS e NIS2, la Legge sul Perimetro di Sicurezza Nazionale Cibernetica, il Digital Services Act (DSA), il Digital Markets Act (DMA), il Data Governance Act (DGA) e il Data Act, il Chips Act europeo e l'AI Act. Queste norme definiscono regole per il controllo delle infrastrutture critiche, la regolazione delle piattaforme globali, la tutela dei dati e il sostegno allo sviluppo industriale.
- **Ruolo di Enti Pubblici e Privati:** il raggiungimento dell'indipendenza digitale coinvolge una molteplicità di attori pubblici (Dipartimento per la Trasformazione Digitale, AgID, ACN, CDP, Ministeri) e privati (operatori di telecomunicazioni, fornitori cloud italiani, industria manifatturiera, università e centri di ricerca). La collaborazione pubblico-privato è fondamentale per allineare priorità strategiche e rafforzare l'ecosistema tecnologico nazionale.
- **Confronto con altri Paesi Europei:** la spinta verso l'indipendenza digitale è un trend europeo. Il rapporto confronta l'Italia con Francia, Germania e Spagna, evidenziando approcci e gradi di maturità diversi nelle strategie cloud, negli investimenti in cybersecurity, nella presenza industriale nazionale e nello sviluppo delle infrastrutture di connettività. Vengono menzionati anche i Paesi nordici e la Polonia per le loro specifiche iniziative.
- **Conclusioni e Prospettive Future:** l'Italia è in un percorso deciso verso una maggiore indipendenza digitale, potenziando infrastrutture e creando poli nazionali come il PSN. L'indipendenza digitale si costruisce anche a livello collettivo europeo. In prospettiva, l'Italia dovrà bilanciare apertura e autonomia, dotandosi di piani di emergenza e salvagenti locali per le tecnologie strategiche. L'obiettivo realistico non è l'autarchia, ma la capacità di scelta autonoma basata sull'interesse nazionale e la consapevolezza dei rischi. Il futuro Libro Bianco approfondirà le analisi e le raccomandazioni operative.

In sintesi, l'indipendenza digitale è un processo continuo che richiede investimenti, normative adeguate, collaborazione pubblico-privato e consapevolezza dei rischi. L'Italia sta compiendo passi importanti in questa direzione, anche nel contesto della cooperazione europea, per garantire un ecosistema digitale sicuro, resiliente e autonomo.

[www.indipendenzadigitale.eu](http://www.indipendenzadigitale.eu)