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

Sommario

Stato delle infrastrutture digitali in Italia 6

Data center nazionali e capacità cloud 6

Analisi settoriale: dipendenze e vulnerabilità specifiche 11

Dipendenza da fornitori esteri nelle tecnologie strategiche 12

La Dimensione Geopolitica..... 12

Rischi Derivanti dalla Dipendenza Tecnologica 15

Iniziative italiane per aumentare il grado di indipendenza digitale 19

Strategia cloud Italia e polo strategico nazionale 19

Gaia-X e iniziative europee di cloud federato 19

Open source e software nazionale 20

Progetti UE di innovazione: HPC, AI e competenze..... 21

Stato della cybersicurezza in Italia e protezione dei dati 22

Capacità di cybersicurezza e minacce..... 22

Tutela dei dati personali e privacy..... 24

Legislazione rilevante per la indipendenza digitale 25

Ruolo di enti pubblici e privati nella transizione digitale e verso l'indipendenza tecnologica 28

Attori pubblici istituzionali 28

Ruolo del settore privato nazionale 29

Confronto con gli altri Paesi Europei sul fronte dell'indipendenza digitale 31

Conclusioni e prospettive future 37

Il Libro Bianco 38
Le dimensioni dell'Indipendenza Digitale 39
La prospettiva dei Governi (UE e Italia) 39
La prospettiva delle Organizzazioni (Enti pubblici e imprese) 40
La prospettiva dei Cittadini 40
I principali assi decisionali per l'indipendenza digitale 40
Le Infrastrutture digitali e la connettività 41
La sicurezza informatica e la protezione dei dati 41
I software sensibili di servizio pubblico 41
Lo sviluppo di standard e soluzioni interoperabili 41
Le aree principali di impatto 42

Premessa

Il presente Rapporto si propone come uno strumento conoscitivo, analitico e critico finalizzato a delineare lo stato dell'arte dell'indipendenza digitale dell'Italia, nella consapevolezza che il digitale rappresenta oggi una dimensione essenziale, trasversale e pervasiva delle infrastrutture materiali e immateriali che sostengono non solo la competitività economica, ma anche l'autonomia politica, la coesione sociale e la garanzia dei diritti fondamentali. Tuttavia, il valore di questo Rapporto non si esaurisce nella sua funzione diagnostica. Esso è concepito sin dall'inizio come parte integrante di un processo più ampio, che vede il suo naturale sbocco nell'elaborazione del **Libro Bianco sull'Indipendenza Digitale dell'Italia**, menzionato nella parte conclusiva del documento. In tal senso, la relazione tra il rapporto e il Libro Bianco è organica e strutturale: il primo svolge la funzione di base conoscitiva, di ricognizione critica delle vulnerabilità e delle potenzialità del sistema paese in materia di autonomia digitale; il secondo, invece, avrà la vocazione esplicitamente propositiva, orientata alla definizione di linee di indirizzo, priorità strategiche, politiche di lungo periodo e strumenti operativi per rafforzare tale indipendenza. Questa relazione può essere ben intesa se adottiamo la distinzione classica tra momento descrittivo-analitico e momento normativo-propositivo. Il rapporto, nella sua natura di documento tecnico e scientifico, si colloca nel primo livello: fornisce una fotografia realistica dello stato delle cose, analizzando infrastrutture, dipendenze critiche, iniziative in corso, confronti internazionali, rischi e minacce emergenti. In questa fase il compito è quello di costruire una rappresentazione il più possibile completa, accurata e fondata empiricamente, evitando anticipazioni prescrittive che potrebbero risultare premature o infondate. Il **Libro Bianco**, invece, si pone a un livello successivo, quello in cui si traduce l'analisi in scelte, si individuano priorità, si formulano raccomandazioni operative. Come ogni libro bianco, esso rappresenterà una piattaforma aperta e dialogica, pensata per stimolare il confronto tra soggetti istituzionali, imprese, società civile, mondo accademico e comunità tecno-scientifica, al fine di promuovere una visione condivisa di indipendenza digitale che non sia fondata su logiche autarchiche o difensive, bensì su un modello di autonomia cooperativa, resiliente, inclusiva e fondata sulla consapevolezza critica.
In questo quadro, il rapporto non è dunque un documento isolato, ma il primo momento di un percorso deliberativo che si concluderà con la stesura del Libro Bianco, inteso come strumento di policy making capace

di tradurre l'analisi in azione, nella consapevolezza che le sfide della sovranità digitale, in un contesto globale interconnesso, esigono visioni strategiche di lungo periodo, scelte coraggiose e un nuovo patto tra istituzioni, cittadini e imprese.

In sintesi, questo rapporto deve essere letto come un **documento preparatorio e propedeutico** al Libro Bianco, volto a garantire che quest'ultimo poggi su basi conoscitive solide, condivise e aggiornate, evitando che le scelte strategiche siano frutto di semplificazioni, narrazioni emergenziali o suggestioni ideologiche. Solo su questa base sarà possibile articolare, nel Libro Bianco, una proposta coerente di rafforzamento dell'indipendenza digitale italiana, capace di conciliare competitività economica, sovranità tecnologica, diritti digitali e sicurezza nazionale.

Introduzione

L'Indipendenza Digitale riguarda la capacità dell'Italia di gestire infrastrutture, dati e tecnologie critiche in modo autonomo, senza eccessive dipendenze o sbilanciamenti potenzialmente rischiosi verso fornitori esteri. Ovviamente, con il termine "indipendenza" non ci si vuole rivolgere al concetto di "autarchia digitale": sia perché ormai anacronistico, soprattutto alla luce del "gap tecnologico" accumulato negli anni del boom della digitalizzazione, sia perché velleitario, in un contesto digitale come quello attuale, concentrato e prestazionalmente quasi irraggiungibile. L'attenzione, dunque, viene posta sulle aree di rischio di una inconsapevole dipendenza digitale e sulle indicazioni necessarie per riuscire a tutelare nel tempo un'indispensabile continuità operativa, a livello europeo, nazionale, imprenditoriale, delle Pubbliche Amministrazioni e verso i cittadini.

In questo Rapporto esaminiamo lo stato delle infrastrutture digitali nazionali, la dipendenza da tecnologie straniere, le iniziative avviate per rafforzare il grado di indipendenza digitale, la situazione della cybersicurezza, il quadro normativo e il ruolo di attori chiave pubblici e privati. Concluderemo con un confronto con altri Paesi europei e una tabella riassuntiva dei principali ambiti strategici potenzialmente oggetto di impatto, evidenziando per ciascuno il grado di indipendenza e i relativi rischi o opportunità.

Lo stato delle infrastrutture digitali in Italia

Le infrastrutture digitali costituiscono la base dell'indipendenza tecnologica di un Paese, poiché garantiscono connettività e capacità di calcolo sotto controllo nazionale. Negli ultimi anni, l'Italia ha investito significativamente per migliorare reti e data center, ottenendo progressi importanti.

I data center nazionali e la capacità cloud

Parallelamente alle reti, l'Italia sta potenziando la propria capacità di calcolo e di cloud sul territorio. Negli ultimi anni c'è stato un vero e proprio boom di data center: i collegamenti di nuove strutture alla rete elettrica in Italia sono aumentati di 40 volte dal 2021, segno dell'espansione rapida dei centri dati. Grandi provider globali hanno aperto regioni cloud in Italia: Amazon Web Services ha lanciato la *region* di Milano nel 2020 (3 data

center) e annunciato ulteriori investimenti per 1,2 miliardi di euro; Microsoft Azure e Google Cloud hanno inaugurato regioni italiane (ad esempio Azure “Italia North” e Google a Milano e Torino) in partnership con attori locali. Invece, Aruba ha recentemente inaugurato il campus Hyper Cloud Data Center a Roma, un ulteriore nodo del network di data center di proprietà del Gruppo Aruba, che comprende il Global Cloud Data Center di Ponte San Pietro (BG) e i due data center di Arezzo.

Le infrastrutture delle Big Tech migliorano i servizi ma fanno capo a multinazionali estere, sollevando il tema del rischio di dipendenza nella gestione dei dati. Per i dati critici del settore pubblico, l’Italia sta implementando il Polo Strategico Nazionale (PSN): un’infrastruttura cloud nazionale, realizzata con fondi PNRR, destinata ad ospitare dati e servizi *strategici* della Pubblica Amministrazione. Il PSN è gestito da una società partecipata da attori italiani (TIM 45%, Leonardo 25%, CDP 20%, Sogei 10%).

Oltre ai grandi provider, è importante evidenziare il ruolo di centinaia di operatori locali e indipendenti, spesso riuniti in associazioni storiche come **AIIP**, che da decenni investono in infrastrutture autonome, comprese reti FTTH proprietarie e data center edge a basso impatto ambientale, altamente interconnessi ai principali backbone nazionali. Questi attori, nonostante la minore visibilità, rappresentano una parte crescente del mercato, come evidenziato anche dai più recenti report AGCOM sulla distribuzione degli accessi ultrabroadband.

Da evidenziare anche il ruolo dell’Italia in infrastrutture strategiche europee di calcolo: presso il Tecnopolo di Bologna è operativo Leonardo, un supercomputer pre-exascale sviluppato in Europa, attualmente il nono più potente al mondo. Leonardo, gestito dal consorzio Cineca, rappresenta un asset critico per l’autonomia tecnologica europea nel calcolo ad alte prestazioni. Inoltre, l’Italia è all’avanguardia anche nell’informatica quantistica grazie a progetti di ricerca connessi a questo supercalcolatore. Queste risorse rafforzano la capacità nazionale di elaborare grandi moli di dati (HPC, AI) senza dover dipendere da centri extraeuropei.

Complessivamente, lo stato delle infrastrutture digitali italiane mostra segnali positivi: accelerazione su fibra e 5G, potenziamento di data center e cloud nazionali, partecipazione a progetti HPC di punta. Resta fondamentale proseguire gli investimenti per coprire le aree scoperte, garantire sicurezza

e assicurare che queste infrastrutture rimangano sotto controllo giurisdizionale italiano/europeo.

I Software, i sistemi operativi e i servizi digitali

L'Italia utilizza massicciamente software e piattaforme sviluppate all'estero, in primis dagli Stati Uniti. Nella Pubblica Amministrazione e nelle imprese sono predominanti sistemi operativi come Windows e Android e suite software di produttività o database fornite, principalmente, da multinazionali USA. Anche i servizi digitali di largo uso – motori di ricerca, social network, messaggistica – sono quasi interamente in mano a Big Tech straniere. Questa situazione comporta ovvi rischi: ad esempio, l'esposizione alle scelte unilaterali di tali aziende o ai cambi normativi dei Paesi d'origine (come il Cloud Act statunitense, che potrebbe imporre l'accesso ai dati degli utenti nonostante siano ospitati in UE). Inoltre, la concentrazione di dati dei cittadini su piattaforme estere pone sfide per privacy e controllo.

L'Italia e l'UE stanno reagendo su due fronti: regolatorio e strategico/industriale. Da un lato, con normative come il GDPR e il Digital Services Act (dettagliato più avanti) si impongono vincoli a Big Tech operanti in Europa, per tutelare dati e diritti degli utenti. Dall'altro, si promuovono (forse un po' tardivamente) alternative europee: ad esempio, l'adozione di software open source nella PA italiana è incoraggiata per ridurre il lock-in verso fornitori proprietari; esiste un Catalogo nazionale del riuso e piattaforme come Developers Italia per condividere soluzioni open source tra Enti. Tuttavia, la quota di mercato di soluzioni interamente "made in Italy" rimane ed è destinata a rimanere minoritaria. Un dato positivo è che il cloud computing – pur dominato dai provider USA – vede anche la presenza crescente di operatori italiani/europei: Aruba, Engineering, TIM Enterprise e Leonardo offrono servizi cloud conformi alle normative UE, puntando sulla governance anche territoriale dei dati (data residency in Italia, cifratura, ecc.). Secondo un'indagine IDC, (*International Data Group*) già il 22% delle organizzazioni italiane utilizza un "cloud sovrano" (erogato da provider nazionali o europei) e un altro 60% di organizzazioni pianifica di adottarlo – segno di una consapevolezza crescente verso soluzioni cloud locali. Resta il fatto che circa il 70% dei ricavi cloud in Europa è assorbito dai colossi USA, una percentuale che sale ulteriormente se consideriamo i servizi SaaS e le piattaforme: una dipendenza strutturale difficile da invertire, nel breve termine.

L’Hardware e i semiconduttori

Un altro tallone d’Achille per l’indipendenza digitale è la filiera hardware e microelettronica. L’Italia (e l’UE) hanno capacità limitate di produzione di chip avanzati e apparecchiature hardware, dipendendo in larga misura da fornitori extraeuropei. I dispositivi ICT utilizzati in Italia – PC, server, smartphone, apparati di rete – provengono in gran parte da fabbriche in Asia (Cina, Taiwan, Corea) o USA. Ciò è emerso in modo critico durante recenti carenze globali di semiconduttori.

Nel settore telecomunicazioni, ad esempio, poche aziende dominano il mercato delle infrastrutture 5G: le europee Ericsson e Nokia e la cinese Huawei (oltre ad alcuni attori minori). L’Italia ha dovuto bilanciare interessi di sicurezza nazionale (limitando Huawei/ZTE nelle reti core 5G con normative specifiche) e necessità di non rallentare la diffusione della rete. Analogamente, per le tecnologie strategiche come server e sistemi di storage la scelta ricade spesso su hardware statunitense (Dell, IBM, HPE) o cinese.

Sul fronte semiconduttori, l’Italia possiede alcune realtà di rilievo, prima fra tutte STMicroelectronics – azienda italo-francese – leader nella produzione di chip per l’automotive, l’industria e componenti di potenza. STMicroelectronics sta investendo in nuove fabbriche in Italia: nel 2022 ha annunciato un impianto da 5 miliardi di euro a Catania per produrre semiconduttori al carburo di silicio (SiC) destinati all’industria automobilistica elettrica, con un co-finanziamento pubblico di 292,5 milioni di euro approvato dalla UE. Questo rientra nell’ambito dell’EU Chips Act, che mira a potenziare la produzione europea di chip. Sempre in ambito Chips Act, l’Italia sta negoziando con Intel la possibile apertura di un impianto avanzato (probabilmente per l’assemblaggio e il packaging di chip) con un investimento di diversi miliardi sostenuto anche da fondi pubblici. Se confermato, sarebbe un passo importante per radicare una filiera microelettronica sul territorio.

Inoltre, l’Italia partecipa a progetti europei IPCEI (Important Projects of Common European Interest) sulla microelettronica. Per esempio nell’IPCEI “Microelectronics and Communication Technologies” vi sono 10 soggetti italiani coinvolti, in diverse applicazioni, con sostegno pubblico. Questi progetti permettono di sviluppare componenti (sensori, chip per telecomunicazioni, semiconduttori di potenza) in cooperazione con partner UE, rafforzando “l’autonomia collettiva” in Europa.

Nonostante queste iniziative, va riconosciuto che nel breve termine la dipendenza dall'estero (fuori Europa) in ambito hardware rimane elevata. Tuttavia, l'Italia sta cercando di mitigare i rischi diversificando fornitori e investendo in capacità nazionali/europee: ad esempio, sperimentando soluzioni Open RAN nelle reti mobili (standard aperti che riducono il vincolo verso pochi vendor proprietari), oppure supportando la ricerca su architetture chip aperte come RISC-V. Queste mosse, da seguire con interesse e attesa, insieme agli investimenti del Chips Act, rappresentano opportunità per recuperare indipendenza tecnologica nella prossima decade.

Indipendenza Digitale nello Spazio

Il tema dell'indipendenza digitale emerge nel contesto della regolamentazione dei lanci e dei servizi via satellite come elemento strategico cruciale per l'autonomia tecnologica e geopolitica dell'Italia e dell'Europa. La frammentazione normativa in ambito europeo è una delle principali criticità: ogni Stato membro regola autonomamente le proprie attività spaziali, in assenza di una licenza unica europea. Questo scenario costringe gli operatori privati europei a confrontarsi con normative differenti, aumentando i costi e le difficoltà operative e rendendo meno competitivo il settore spaziale europeo rispetto a USA e Cina.

L'Unione Europea, pur avendo una politica spaziale comune (TFUE art. 189), non può armonizzare le normative nazionali, limitandosi a fornire indirizzi strategici e programmi di sostegno, come il Programma Spaziale UE 2021-2027, che finanzia infrastrutture critiche per la navigazione satellitare, l'osservazione terrestre e la sicurezza. Tuttavia, l'assenza di un quadro normativo uniforme indebolisce l'indipendenza industriale europea in un settore considerato sempre più centrale per la sicurezza nazionale, il controllo delle comunicazioni e la gestione dei dati strategici.

L'Europa ha promosso iniziative per sviluppare capacità di lancio autonome (Ariane, Vega), ma resta vulnerabile nei confronti di operatori extra-europei per quanto riguarda componenti critiche, tecnologie dual-use e gestione del traffico spaziale (STM). Anche le politiche di contrasto alla congestione orbitale e ai detriti spaziali sono ancora in fase embrionale, con il rischio di dipendere da sistemi di sorveglianza statunitensi o cinesi.

In questo scenario, l'Italia ha avviato un processo di rafforzamento interno con il DDL Economia dello Spazio 2025, che mira a consolidare una

governance nazionale capace di dialogare con le istituzioni europee e internazionali, proponendosi come modello per la futura definizione di un European Space Act. Tale iniziativa, se attuata, potrebbe mitigare la dipendenza normativa e industriale dell'Europa dagli attori globali dominanti, favorendo una maggiore sovranità tecnologica e digitale.

Il nodo centrale resta quindi la tensione tra un sistema normativo nazionale e frammentato e l'esigenza di costruire un mercato unico europeo dello spazio che garantisca indipendenza tecnologica e autonomia decisionale nel contesto della geopolitica digitale globale.

Un'analisi settoriale: dipendenze e vulnerabilità specifiche

Nel contesto della crescente digitalizzazione, alcuni "settori chiave" come Energia, Trasporti, Sanità, Finanza e Comunicazioni mostrano una crescente esposizione a dipendenze tecnologiche critiche e vulnerabilità digitali. Queste fragilità, spesso si intrecciano con interdipendenze cross-settoriali complesse e possono amplificare i rischi sistemici, compromettendo la capacità di tutela delle infrastrutture essenziali.

- **Energia:** il settore energetico europeo dipende da hardware e software importati per la gestione delle reti (SCADA/ICS), lo sviluppo delle smart grid e le infrastrutture per le energie rinnovabili (pannelli solari e turbine eoliche spesso provengono dalla Cina). I sistemi di controllo operativo (OT) presentano vulnerabilità specifiche e la sicurezza dell'approvvigionamento energetico è a rischio a causa di possibili interruzioni della catena di fornitura o attacchi mirati. Infrastrutture fisiche come gasdotti, cavi sottomarini e centrali elettriche sono esposte a minacce sia fisiche che informatiche. La Germania, con il suo quadro KRITIS, offre esempi concreti delle sfide nella protezione di questo settore.
- **Trasporti**: i sistemi di trasporto moderni (controllo del traffico aereo, segnalamento ferroviario, gestione del traffico stradale - ITS, logistica, veicoli autonomi) sono intrinsecamente dipendenti da complesse infrastrutture digitali. I rischi includono la compromissione dei sistemi di navigazione satellitare (GPS/Galileo), attacchi alle reti di comunicazione utilizzate per il controllo e la potenziale interruzione delle catene logistiche globali a causa di incidenti informatici o fisici. Progetti come RESIIST in

Francia evidenziano la necessità di strategie di resilienza specifiche per questo settore.

- **Sanità**: il settore sanitario fa crescente affidamento su dispositivi medici connessi (IoT), cartelle cliniche elettroniche (EHR), sistemi informativi ospedalieri e piattaforme cloud per l'analisi e l'archiviazione dei dati. Le vulnerabilità includono attacchi ransomware che paralizzano gli ospedali [6], violazioni di dati sanitari sensibili e la compromissione di dispositivi medici impiantabili o utilizzati per terapie critiche. La strategia italiana pone un focus su questo settore.
- **Finanza**: le operazioni bancarie, i sistemi di pagamento, le infrastrutture dei mercati finanziari e la gestione del rischio dipendono in modo critico dalle tecnologie dell'informazione e della comunicazione (ICT), con un uso crescente di servizi cloud. Regolamenti specifici come DORA mirano ad affrontare la resilienza operativa digitale. I rischi principali sono il furto di dati finanziari e l'interruzione dei servizi, che possono avere impatti sistemici sull'economia.
- **Comunicazioni**: questo settore è fondamentale in quanto abilita la digitalizzazione di tutti gli altri. Le dipendenze da fornitori extra-UE per le infrastrutture 5G e altre reti, i cavi sottomarini, le comunicazioni satellitari e le infrastrutture cloud/data center sono particolarmente pronunciate. I rischi riguardano la disponibilità (interruzioni), l'integrità (manipolazione dei dati) e la riservatezza (spionaggio) delle comunicazioni.
- **Interdipendenze cross-settoriali che possono amplificare i rischi**: le vulnerabilità non sono confinate all'interno dei singoli settori. Data la profonda interconnessione delle infrastrutture critiche moderne, un'interruzione in un settore fondamentale come l'energia (spesso fortemente dipendente da tecnologie extra-UE) o le comunicazioni può innescare effetti a cascata che si propagano rapidamente ad altri settori come la sanità, la finanza, i trasporti e la pubblica amministrazione. Questo significa che un singolo punto di fallimento o un attacco mirato a un'infrastruttura digitale dipendente da fornitori esterni può avere conseguenze sistemiche, amplificando enormemente l'impatto potenziale e mettendo a rischio il funzionamento dell'intera società.

La dipendenza da fornitori esteri nelle tecnologie strategiche

La Dimensione Geopolitica

La dipendenza tecnologica da attori esterni con interessi strategici potenzialmente (o sorprendentemente) divergenti rappresenta una fonte crescente di vulnerabilità. **Un percorso di consapevolezza passa dall'identificazione di chi considerare amico e chi rivale in ambito geopolitici, per poi affrontare la completezza dei quadri giuridici, le aree di influenza presidiabili e i rischi e le minacce di una dipendenza digitale.**

- Identificazione dei Rivali: nel contesto dei rischi tecnologici per le infrastrutture critiche, Cina e Russia sono frequentemente citate come rivali geopolitici o paesi con sistemi politici e normativi divergenti che presentano rischi specifici per l'UE. La dipendenza tecnologica da aziende con sede in questi paesi è vista come una vulnerabilità strategica.
- Quadri Giuridici e Politici: leggi nazionali specifiche in paesi rivali, come la Legge sull'Intelligence Nazionale cinese del 2017, possono obbligare le aziende (anche private) con sede legale nel loro territorio a cooperare con i servizi di intelligence e sicurezza statali. Questo quadro legale alimenta i timori che tali aziende possano essere utilizzate come vettori per attività di spionaggio o sabotaggio contro infrastrutture critiche europee.
- Influenza Statale: nei sistemi autoritari, la distinzione tra settore privato e influenza statale può essere labile. Esiste il rischio che governi stranieri esercitino un controllo diretto o indiretto sulle aziende tecnologiche, anche quelle nominalmente private, per perseguire obiettivi strategici o di sicurezza nazionale a scapito degli interessi europei.
- Minacce Ibride: la dipendenza tecnologica si inserisce nel contesto più ampio delle minacce ibride. Attori statali o loro proxy possono sfruttare le vulnerabilità tecnologiche come parte di campagne più vaste che includono disinformazione, coercizione economica, attacchi informatici e sabotaggio fisico per destabilizzare l'UE o singoli Stati membri.
- La Dipendenza digitale come leva strategica (degli altri): la dipendenza tecnologica da aziende soggette a influenze geopolitiche avverse non è solo una vulnerabilità passiva, ma si traduce direttamente in una potenziale leva strategica per chi si comporta da "rivale". Questa leva può essere sfruttata attraverso vari mezzi – spionaggio facilitato da accessi tecnici, sabotaggio remoto di infrastrutture, interruzione mirata delle forniture o aggiornamenti, o coercizione economica e politica basata sulla minaccia di tali azioni. La dipendenza tecnologica diventa così uno

strumento geopolitico che minaccia direttamente la sicurezza europea, l'integrità delle sue infrastrutture critiche e la sua autonomia decisionale.

Complessità delle Catene di Approvvigionamento Globali

Il grado di “dipendenza” delle infrastrutture critiche dipende in larga misura anche dall’affidabilità delle “supply chain” tecnologiche, oggi caratterizzate da una elevata e intricata complessità globale. La frammentazione, l'opacità e la vulnerabilità intrinseca di queste supply chain espongono Governi, Stati, Imprese, PA e cittadini a rischi trasversali, spesso difficili da individuare o mitigare tempestivamente.

- Interconnessione Globale: le catene di approvvigionamento tecnologico (supply chain) per semiconduttori, componenti hardware, software e servizi sono estremamente complesse, globalmente distribuite e interconnesse. Nessuna “regione”, attualmente, è completamente autosufficiente.
- Mancanza di trasparenza: la natura multi-livello e geograficamente dispersa delle supply chain rende difficile ottenere una visibilità completa e un controllo end-to-end. È complesso verificare l'integrità e la sicurezza di ogni singolo componente o processo lungo l'intera catena.
- Punti di vulnerabilità: le catene di approvvigionamento presentano molteplici punti in cui possono essere introdotte vulnerabilità o compromissioni, sia intenzionalmente che accidentalmente: nella fase di progettazione, durante la produzione, nella distribuzione, tramite aggiornamenti software/firmware o durante la manutenzione. I rischi possono derivare non solo dal fornitore principale, ma anche dai suoi subfornitori (terze parti) o dall'uso di componenti software open-source vulnerabili.
- Colli di bottiglia geopolitici: tensioni geopolitiche, sanzioni (come quelle statunitensi contro Huawei, ma anche come le scosse di assestamento e riassetto degli equilibri storici, introdotte nell’ultimo periodo nel commercio internazionale), controlli sulle esportazioni, conflitti armati o disastri naturali possono interrompere bruscamente le catene di approvvigionamento. Questo può bloccare la fornitura di hardware, software o aggiornamenti essenziali, impattando la capacità di implementare, mantenere e rendere resilienti le infrastrutture critiche.
- La Sicurezza della Supply Chain è una sfida fondamentale: la complessità intrinseca, l'opacità e la distribuzione globale delle catene di approvvigionamento tecnologico rappresentano un rischio fondamentale e pervasivo per le infrastrutture critiche, indipendentemente dall'origine

specifica di ciascun fornitore finale locale. Anche se un fornitore primario è considerato "affidabile", i rischi possono emergere dai suoi fornitori di secondo o terzo livello, e – come spesso è accaduto di recente - da componenti software integrati. Questo rende la sicurezza della supply chain un'ulteriore sfida distinta e fondamentale, che richiede attenzioni dedicate capaci di andare oltre il semplice screening dei fornitori finali, come quelle contemplate nella Direttiva NIS2 o nel Cyber Resilience Act.

Nonostante i progressi infrastrutturali, l'Italia – come l'Europa intera – risente di una forte dipendenza da fornitori esteri in vari ambiti chiave dell'ecosistema digitale. Questo rappresenta un potenziale fattore di vulnerabilità per la indipendenza tecnologica. Esaminiamo le aree principali di dipendenza: software e servizi cloud, hardware e semiconduttori.

I rischi derivanti dalla dipendenza tecnologica

Tra i rischi più rilevanti della dipendenza da tecnologie non presidiabili direttamente o "fuori controllo", emergono lo spionaggio informatico, l'esfiltrazione di dati sensibili e non, i sabotaggi e forme di coercizione economica e politica legate al controllo delle forniture di servizi, reti e accessi ad altre infrastrutture digitali.

- **Spionaggio Informatico ed Esfiltrazione di Dati**
  - Motivazioni: lo spionaggio informatico contro le infrastrutture critiche è motivato dal desiderio di rubare proprietà intellettuale, ottenere vantaggi politici o economici, raccogliere informazioni operative dettagliate sulle infrastrutture stesse, potenzialmente per pianificare futuri attacchi o sabotaggi o semplicemente per minare la reputazione di un "brand", sia esso un'istituzione pubblica o un attore privato.
  - Fattori di e rischio della dipendenza digitale: la dipendenza da tecnologie extra-UE può creare molteplici falle che prestano il fianco allo spionaggio:
    - Backdoor/Vulnerabilità: esiste il rischio che hardware o software forniti da aziende soggette all'influenza di governi stranieri contengano punti di accesso nascosti (backdoor) o vulnerabilità deliberatamente introdotte, utilizzabili per l'accesso non autorizzato.
    - Accesso ai dati (cloud): il rischio più significativo riguarda l'accesso da parte di governi stranieri a dati sensibili relativi

alle infrastrutture critiche (dati operativi, dati dei cittadini) archiviati presso fornitori di servizi cloud extra-UE. Leggi come il CLOUD Act statunitense possono facilitare legalmente tale accesso, aggirando le normative europee sulla protezione dei dati.
        - Manutenzione/Aggiornamenti: operazioni di manutenzione remota o aggiornamenti software eseguiti da fornitori extra-UE o loro subappaltatori rappresentano un'opportunità potenziale per insinuare codice malevolo o esfiltrare dati.

    - Impatto sulle infrastrutture critiche: le conseguenze dello spionaggio possono essere gravi, come per esempio la perdita di piani operativi strategici, l'esposizione di vulnerabilità sfruttabili per attacchi futuri, la compromissione di dati personali sensibili relativi a servizi essenziali (sanità, finanza). Non va tralasciato che ciascuno di questi danni, oltre al proprio impatto diretto, contribuisce anche a minare la fiducia dei cittadini nella sicurezza nazionale.
    - I dati come obiettivo primario: nel contesto della protezione delle infrastrutture critiche e dell'indipendenza digitale, i dati – siano essi operativi, personali o strategici – costituiscono un obiettivo primario per azioni di spionaggio. Le infrastrutture critiche generano e processano enormi quantità di dati sensibili. La dipendenza da fornitori extra-UE, in particolare per i servizi cloud e le reti di comunicazione, crea percorsi significativi per l'esfiltrazione di questi dati. Leggi straniere [come il CLOUD Act] o la potenziale compromissione dei fornitori (tramite backdoor o coercizione) possono consentire l'accesso a servizi di intelligence stranieri, anche in modalità intermediata, tornando al tema delle supply chain tecnologiche. Pertanto, la dipendenza tecnologica facilita direttamente lo spionaggio incentrato sui dati contro le infrastrutture critiche, minando sia la loro sicurezza operativa sia la capacità di disporre e governare in autonomia le informazioni da parte dell'Europa.
- **Sabotaggio e Interruzione dei Servizi**
    - Motivazioni: il sabotaggio delle infrastrutture critiche può essere motivato da obiettivi geopolitici (esercitare pressione, destabilizzare un avversario, minarne la reputazione), economici (paralizzare l'economia di un rivale) o militari (supportare operazioni cinetiche degradando le capacità del nemico).

- **Fattori di rischio legati alla dipendenza:** la dipendenza tecnologica offre ampie opportunità di sabotaggio:
  - Spegnimento/manipolazione remota: fornitori extra-UE, potenzialmente sotto direttiva statale, potrebbero avere la capacità tecnica di disabilitare o manipolare, da remoto, componenti critici delle reti (es. stazioni base 5G, funzioni core della rete, reti satellitari) o sistemi di controllo industriale (ICS/OT) che governano processi fisici.
  - Aggiornamenti malevoli: l'iniezione di malware distruttivo tramite aggiornamenti software o firmware provenienti da fornitori compromessi o costretti a cooperare può concretizzarsi in un rischio concreto.
  - Sfruttamento di vulnerabilità note: vulnerabilità note (o deliberatamente introdotte e non divulgate) in apparecchiature ampiamente diffuse e non controllabili possono essere sfruttate per causare interruzioni su larga scala.
- Impatto sulle Infrastrutture Critiche: le conseguenze del sabotaggio possono essere catastrofiche, dai blackout elettrici estesi, alle paralisi delle reti di trasporto, dall'interruzione delle comunicazioni, al blocco dei servizi finanziari, dalla contaminazione delle forniture idriche all'interruzione dei servizi sanitari. Incidenti reali come gli attacchi alla rete elettrica ucraina, l'attacco a Viasat o il sabotaggio del Nord Stream denotano la gravità potenziale.
- Potenziale di disgregazione sistemica: le dipendenze tecnologiche, specialmente nelle funzioni centrali delle reti e nei sistemi di controllo industriale, conferiscono a potenziali avversari la capacità di infliggere interruzioni diffuse e sistemiche che possono propagarsi rapidamente attraverso molteplici settori critici interconnessi. Un attacco mirato a un componente digitale chiave, reso possibile dalla dipendenza da un fornitore esterno, può innescare effetti a cascata, mettendo a rischio il funzionamento dell'intera società e rappresentando una minaccia esistenziale per la stabilità nazionale ed europea.

- **Integrità nelle Catene di Approvvigionamento:**
  - Manomissione (Tampering): esiste il rischio che componenti hardware o software malevoli vengano inseriti in qualsiasi punto delle complesse supply chain tecnologiche dei servizi e delle infrastrutture digitali. Questo può avvenire durante la progettazione, la produzione o la distribuzione, potenzialmente ad

opera di attori che mirano a compromettere specifici fornitori o componenti, anche agendo prima che raggiungano il mercato europeo.

- Interruzione: eventi geopolitici (conflitti, instabilità), sanzioni, controlli sulle esportazioni, disastri naturali o azioni deliberate da parte di uno stato che controlla un fornitore chiave possono interrompere la fornitura di hardware, software o aggiornamenti necessari. Ciò può impattare direttamente la capacità di implementare, mantenere e rendere resilienti le infrastrutture critiche.
- **Vendor Lock-in: la dipendenza da tecnologie proprietarie di un singolo fornitore, o di un numero limitato di essi, può creare una situazione di "vendor lock-in". Questo riduce le possibilità di scelta, potenzialmente aumenta i costi, ostacola l'innovazione endogena e rende estremamente difficile e costoso cambiare fornitore, anche qualora emergessero gravi rischi per la sicurezza o se la situazione geopolitica mutasse sfavorevolmente.**
- Impatto sulle Infrastrutture Critiche: i rischi legati alle catene di approvvigionamento compromettono direttamente la capacità di costruire, mantenere, proteggere e aggiornare le infrastrutture critiche in modo affidabile e sicuro nel lungo periodo, minando la pianificazione strategica e la resilienza.
- Il rischio della Supply Chain mina la resilienza a lungo termine: oltre alle minacce immediate di spionaggio o sabotaggio, le vulnerabilità intrinseche delle catene di approvvigionamento (manomissione, interruzione, lock-in) derivanti dalla dipendenza tecnologica rappresentano una minaccia strategica alla resilienza e all'adattabilità a lungo termine delle infrastrutture critiche. Queste vulnerabilità ostacolano la capacità di qualsiasi Sistema di perimetrare correttamente i confini entro i quali affrontare le proprie verifiche di continuità e sicurezza, di far evolvere in modo sicuro le proprie infrastrutture, di integrare nuove tecnologie e di rispondere efficacemente alle sfide future, siano esse tecnologiche, geopolitiche o ambientali. La sicurezza della supply chain diventa quindi un prerequisito fondamentale per adottare un approccio sostenibile.

- **Coercizione Economica e Politica**

- Sfruttare la Dipendenza: una posizione dominante in tecnologie critiche (es. 5G, cloud, semiconduttori, IA) può essere utilizzata da uno stato extra-UE, agendo direttamente o tramite le sue aziende, per esercitare pressioni economiche o politiche sull'UE o sui suoi Stati membri.
- Scenari di coercizione: potenziali tattiche coercitive includono la minaccia di ritirare tecnologie o servizi essenziali, l'imposizione di aumenti di prezzo significativi e ingiustificati (in qualche caso, già visibili nelle esperienze del quotidiano con i servizi in cloud), il condizionamento dell'accesso al mercato o della fornitura tecnologica all'allineamento strategico, o l'uso del controllo tecnologico per influenzare decisioni politiche nazionali.
- Strumentalizzazione della tecnologia: la dipendenza tecnologica non crea solo rischi di azioni segrete come spionaggio e sabotaggio, ma abilita anche forme di coercizione economica e culturale più “aperte”. La possibilità che uno stato che smette di essere amico possa "spegnere" o degradare servizi digitali critici, o possa anche solo minacciare di farlo, conferisce a tale stato una potente leva negoziale. Questo trasforma la tecnologia stessa, ormai diventata strategicamente indispensabile, in un potenziale strumento di potere geopolitico, minando direttamente l'autonomia e la libertà decisionale di un territorio.

Le iniziative italiane per aumentare il grado di indipendenza digitale

Conscio delle criticità sopra descritte, il sistema-Paese italiano ha messo in campo diverse iniziative strategiche per rafforzare la propria indipendenza digitale. Si tratta sia di progetti autonomi nazionali, sia della partecipazione attiva a programmi europei condivisi. Di seguito analizziamo i principali.

La strategia cloud italiana e il Polo Strategico Nazionale

Gaia-X e le iniziative europee di cloud federato

A livello europeo, l’Italia partecipa al progetto Gaia-X, lanciato nel 2020 da Francia e Germania e poi allargato ad altri Paesi membri, con l’intento di creare un ecosistema cloud federato europeo. Gaia-X non è un provider cloud singolo, bensì un framework di standard e interoperabilità per

consentire a dati e servizi di muoversi tra cloud diversi con garanzie di reversibilità, trasparenza e controllo da parte degli utenti. L'idea chiave è favorire una rete di cloud nazionali interoperabili secondo regole comuni ("federated cloud"), riducendo la dipendenza dalle Big Tech attraverso la cooperazione paneuropea. L'Italia ha istituito il Gaia-X Hub nazionale, coinvolgendo aziende e centri di ricerca per sviluppare casi d'uso nei settori agrifood, finanza, industria 4.0, energia, etc., che potrebbero beneficiare della condivisione sicura di dati tra partner europei.

Sebbene Gaia-X abbia incontrato ritardi e alcuni scetticismi, ha stimolato riflessioni importanti sul controllo dei dati: l'obiettivo dichiarato è creare "un'infrastruttura di dati che rispecchi i valori europei di autonomia e auto-determinazione, garantendo la sovranità dei dati". L'impegno italiano in Gaia-X si affianca ad altre iniziative UE come la European Alliance for Industrial Data and Cloud e l'EU Cloud Rulebook, con cui la Commissione mira a definire certificazioni di "cloud di fiducia" (EU Trust Cloud) privilegiando fornitori che rispettino requisiti di localizzazione dei dati e indipendenza da legislazioni extra-UE.

Un ulteriore progetto europeo di cui l'Italia è protagonista è l'IPCEI Cloud & Edge, approvato dalla Commissione nel 2022, che finanzia con fondi pubblici lo sviluppo di nuove soluzioni cloud ed edge computing europee. Inoltre, aziende italiane (ad es. Leonardo e Aruba) sono coinvolte per creare servizi cloud innovativi e compatibili con Gaia-X. L'insieme di queste iniziative (Gaia-X, IPCEI, EUCS certification) punta a costruire nel medio termine un "Eurocloud" competitivo: una rete di provider e infrastrutture *made in EU* su cui cittadini, imprese e governi possano fare affidamento sapendo che i dati restano sotto giurisdizione europea.

Open source e software nazionale

Un aspetto a volte meno citato, ma rilevante per l'indipendenza digitale, è la promozione di software open source e standard aperti. L'Italia già dal 2012 con il Codice dell'Amministrazione Digitale prevede l'obbligo per le PA di valutare soluzioni open source prima di acquistare software proprietario. Negli ultimi anni, progetti come Developers Italia (community lanciata da AgID) e Docs Italia hanno incentivato la condivisione di codici e applicativi pubblici. Ad esempio, **il sistema IO (l'app dei servizi pubblici), l'ANPR (Anagrafe nazionale) o la piattaforma pagoPA sono sviluppati con contributi open e riutilizzabili da altre**

amministrazioni. Ciò aumenta l'indipendenza dalla singola software house fornitrice e consente a sviluppatori italiani di contribuire/mantenere il codice.

Anche grandi aziende nazionali hanno puntato su tecnologie aperte: Aruba, ad esempio, ha costruito la propria offerta cloud su stack open source (come OpenStack, Kubernetes) per evitare lock-in tecnologici, e sottolinea che l'indipendenza digitale è un elemento chiave riconosciuto anche dagli analisti per i provider operativi in Europa. Promuovere formati aperti, protocolli standard, open software significa poter sostituire un componente tecnologico con alternative equivalenti, senza restare vincolati a un unico fornitore straniero. Questo approccio "open" è dunque parte integrante delle strategie di autonomia digitale.

I progetti UE di innovazione: HPC, AI e competenze

Infine, l'Italia partecipa a numerose iniziative europee che, pur non riferendosi esplicitamente alla "indipendenza digitale", ne condividono gli obiettivi. Oltre ai citati Gaia-X e IPCEI, ricordiamo:

- EuroHPC: oltre al supercomputer Leonardo, l'Italia partecipa al network europeo di calcolo ad alte prestazioni e ospiterà uno dei primi computer quantistici europei integrati in tale rete. Disporre di capacità di calcolo proprie è essenziale per l'indipendenza scientifica e industriale (simulazioni, clima, difesa, ecc.).
- Programma Digital Europe: finanziamenti UE per creare poli di innovazione digitale (in Italia ne sono stati selezionati 13) e progetti su AI, cybersecurity, competenze digitali avanzate. Questi programmi aiutano l'ecosistema italiano a sviluppare *know-how* locale in tecnologie emergenti, riducendo la necessità di importare soluzioni dall'estero.

- Alleanze su AI e microelettronica: l'Italia aderisce alle alleanze europee sull'intelligenza artificiale e sui processori (European AI Alliance, Alliance on Processors and Semiconductor technologies) per condividere risorse e fissare obiettivi comuni, ad esempio sulla prossima generazione di chip low-power o sull'AI etica e affidabile. In ambito AI, va citata la collaborazione rafforzata avviata nel 2023 tra Italia, Francia e Germania per progetti comuni di ricerca e standardizzazione sull'intelligenza artificiale e il cloud "di fiducia" europeo.

Queste iniziative mostrano una chiara direzione: fare sistema a livello nazionale ed europeo per sviluppare alternative tecnologiche all'import, in modo cooperativo. **L'indipendenza digitale dell'Italia, infatti, non può prescindere dal contesto comunitario: solo attraverso massa critica e visione comune, l'Europa (di cui l'Italia è parte integrante) può aspirare a un ruolo autonomo nell'era digitale.**

Lo stato della cybersicurezza in Italia e la protezione dei dati

L'indipendenza digitale non riguarda solo infrastrutture e fornitori, ma anche la capacità di proteggere efficacemente il cyberspazio nazionale e i dati dei cittadini. Un Paese tecnologicamente non-dipendente deve saper tutelare le proprie reti da minacce informatiche esterne e garantire la privacy delle informazioni secondo le proprie leggi. In questo ambito, l'Italia ha compiuto passi da gigante di recente, pur essendo comunque chiamata ad affrontare sfide ancora importanti e crescenti (in analogia, peraltro, con molti altri Paesi Europei).

La capacità di cybersicurezza e le minacce

Negli ultimi anni l'Italia ha costruito un solido sistema di governance della cybersecurity, riconosciuto anche a livello internazionale. Nel Global Cybersecurity Index 2024 dell'ITU, l'Italia si colloca nel gruppo di testa (Tier 1) con un punteggio fra 95 e 100 su 100 (segno di un forte impegno coordinato nel tempo dal governo). Questo risultato è frutto di importanti riforme: la creazione dell'Agenzia per la Cybersicurezza Nazionale (ACN) nel 2021 ha centralizzato competenze prima frammentate, dotando il Paese di un organismo dedicato alla supervisione della strategia cyber. L'ACN funge da punto di contatto unico per le emergenze cyber, supporta le amministrazioni nell'innalzare i livelli di sicurezza e coordina il CSIRT Italia (Computer Security Incident Response Team).

Parallelamente, è stato definito un robusto perimetro di sicurezza cibernetica nazionale (legge 133/2019) che impone obblighi di sicurezza stringenti ai soggetti – pubblici e privati – che gestiscono infrastrutture critiche. Questi enti devono adottare misure minime, notificare incidenti e sottoporre a valutazione governativa (Golden Power) l'acquisizione di tecnologie ICT critiche provenienti da Paesi extra-UE. Tali misure mirano a scongiurare

inserimenti di backdoor o dipendenze non controllate in asset sensibili (es. reti energetiche, telecomunicazioni, difesa).

Nonostante questi progressi sul piano normativo-organizzativo, la minaccia cyber anche in Italia è in costante aumento. I report di ACN indicano un'impennata di attacchi: solo nel 2023, il CSIRT Italia ha gestito 3.302 incidenti informatici gravi, quasi il triplo rispetto ai 1.150 del 2022. L'Italia risulta bersaglio frequente di campagne globali di ransomware e phishing, posizionandosi al poco apprezzabile 1° posto in UE per attacchi ransomware a metà 2024. E in tutto il 2024 il CSIRT Italia ha gestito 1.979 eventi cyber, ben 165 al mese: di questi sono 573 gli incidenti con impatto confermato. Rispetto al 2023 gli eventi sono aumentati del 40% e gli incidenti quasi del 90%. Settori come la PA, la sanità e le supply chain di aziende italiane sono stati colpiti da attacchi sempre più sofisticati, volti a sottrarre dati strategici e know-how industriale ma anche a minare la reputazione di chi non è riuscito ad evitare i rischi. Questa situazione evidenzia come la capacità difensiva vada ulteriormente potenziata e la consapevolezza di quale sia stato "l'anello debole della catena" costantemente sensibilizzata: secondo ACN, l'Italia soffre ancora di una carenza di specialisti e competenze cyber in molti enti, e deve "cambiare marcia" per tenere il passo con la crescita esponenziale delle minacce.

Le strategie nazionali recentemente adottate puntano proprio a rafforzare la resilienza: la Strategia Nazionale di Cybersicurezza 2022-26, elaborata da ACN, prevede 82 misure, di cui 69 già avviate, da raggiungere entro il 2026, tra cui, l'innalzamento delle difese in tutti i settori critici, programmi di formazione cyber per 300.000 addetti della PA e lo sviluppo di tecnologie crittografiche ed endpoint nazionali in ambito governativo. Inoltre, con l'entrata in vigore della direttiva NIS2 (recepita in Italia col D.Lgs. 138/2024), molte più aziende di interesse pubblico (trasporti, finanziario, fornitura digitale, ecc.) sono chiamate a rispettare standard di sicurezza comuni e notificare incidenti. L'ACN è stata designata autorità competente NIS e sta guidando l'adeguamento di questi operatori.

In termini di difesa attiva, l'Italia partecipa a cooperazioni europee come l'European Cybersecurity Competence Centre (ECCC): l'ACN è National Coordination Centre per l'Italia, contribuendo a progetti di ricerca e sviluppo in ambito sicurezza (es. tecnologie di cybersicurezza avanzate da usare anche a fini militari e di intelligence). Non va dimenticata, infine, l'attenzione crescente alla sicurezza dei fornitori ICT stranieri: il governo esercita regolarmente il Golden Power sulle forniture TLC (negli ultimi anni

sono stati posti veti o condizioni a contratti con Huawei e ZTE per reti 5G core e backbone) e ha stilato elenchi di produttori "certificati" per la PA. Questa vigilanza riduce il rischio di backdoor in attrezzature di rete e consolida l'autonomia decisionale su quali tecnologie impiegare.

La tutela dei dati personali e la privacy

Un elemento centrale di indipendenza digitale è il controllo sui dati personali dei cittadini. In questo ambito l'Italia beneficia del forte quadro normativo europeo: il GDPR (Regolamento Generale sulla Protezione dei Dati) è in vigore dal 2018 e ha imposto standard elevati e omogenei a tutte le imprese, incluse le Big Tech, riguardo al trattamento dei dati. Il GDPR è stato attuato in Italia aggiornando il Codice Privacy nazionale (D.Lgs. 101/2018). L'azione combinata del Garante Privacy italiano e del Comitato Privacy europeo ha portato a sanzioni significative verso colossi come Google, Meta e Microsoft per violazioni, affermando nei fatti l'indipendenza regolamentare europea sul cyberspazio. Un esempio emblematico è stato nel 2023 il provvedimento del Garante che ha temporaneamente sospeso ChatGPT per mancato rispetto delle norme privacy, costringendo la società OpenAI (USA) ad adeguarsi alle richieste italiane prima di poter riprendere il servizio nel nostro Paese – un chiaro segnale della capacità di enforcement nazionale anche verso attori globali.

Oltre al GDPR, altre norme contribuiscono alla tutela dei dati: il *Regolamento per le infrastrutture digitali e per i servizi cloud per la pubblica amministrazione* (adottato da ACN con Decreto Direttoriale n. 21007/24 del 27 giugno 2024 e applicabile dal 1 agosto 2024), richiede che i dati pubblici siano allocati in modo conforme a principi di sicurezza, cybersicurezza e privacy; il Regolamento UE sui dati non personali garantisce libera circolazione dei dati aziendali in Europa ma proibisce restrizioni extraterritoriali (in risposta ad esempio a leggi come il Cloud Act USA). Inoltre, è in arrivo il Data Act europeo che disciplinerà accesso e condivisione dei dati industriali e IoT, e l'AI Act che imporrà criteri di trasparenza sugli algoritmi: entrambe mirano a far sì che l'uso dei dati in UE avvenga secondo regole decise democraticamente dagli europei stessi, e non dalle sole logiche di mercato proposte o imposte dalle multinazionali.

In termini di dati pubblici, l'Italia aderisce al principio che "i dati dei cittadini sono una risorsa nazionale". Progetti come la Piattaforma Digitale

Nazionale Dati (PDND) e le iniziative di open data puntano a valorizzare il patrimonio informativo pubblico sul territorio nazionale, evitando che finisca raccolto e sfruttato esclusivamente da soggetti esteri. Anche le partnership internazionali sui dati vengono valutate con attenzione: ad esempio, per il trattamento di dati sanitari il Ministero ha privilegiato soluzioni cloud in ambito UE, in linea col progetto European Health Data Space.

In definitiva, sul fronte cybersicurezza e dati, l'Italia sta cercando di coniugare apertura digitale e orientamento all'indipendenza: da un lato incoraggiando l'uso diffuso di servizi digitali (anche stranieri), dall'altro ponendo regole chiare a tutela dell'interesse nazionale e dell'utente. La sicurezza cibernetica è parte integrante della necessaria indipendenza digitale per il sistema Paese, per le organizzazioni pubbliche e private così come per i cittadini che ne fanno parte: in un mondo ormai quasi completamente digitale, infatti, proteggere infrastrutture e dati significa preservare l'autonomia, la sicurezza e la continuità operativa del Paese.

La legislazione rilevante per l'indipendenza digitale

Il quadro normativo, sia italiano che europeo, è un fattore abilitante cruciale della indipendenza digitale. Leggi e regolamenti definiscono confini, obblighi e diritti nello spazio digitale, permettendo all'Italia di esercitare la propria autorità su infrastrutture e dati. Ecco una panoramica delle principali normative in vigore o in arrivo legate al tema:

- Regolamento Generale sulla Protezione dei Dati (GDPR) – UE, 2016/679: pilastro della tutela dei dati personali in Europa. Garantisce che i dati dei cittadini italiani (e UE) siano trattati secondo rigorosi standard di privacy, indipendentemente da dove abbia sede l'azienda che li gestisce. **Il GDPR ha reso gli Stati UE "sovrani" nel poter sanzionare aziende globali sul loro operato con i dati degli europei. In Italia è applicato tramite il D.Lgs. 101/2018.**

- Direttiva NIS e NIS2 – UE 2016/1148 e 2022/2555: normative sulla sicurezza delle reti e dei sistemi informativi. La prima direttiva NIS (recepita in Italia col D.Lgs. 65/2018) ha introdotto requisiti minimi di sicurezza informatica per operatori di servizi essenziali; la NIS2, aggiornata nel 2022 e recepita con D.Lgs. 138/2024, amplia notevolmente

il campo di applicazione e impone regole più severe. Settori come energia, trasporti, finanza, sanitario, infrastrutture digitali, fornitura ICT, pubblica amministrazione, sono tutti coinvolti. Ciò rende obbligatoria una postura cyber elevata su gran parte del tessuto economico nazionale, diminuendo le vulnerabilità sistemiche.

- Legge 133/2019 – Perimetro di Sicurezza Nazionale Cibernetica: normativa italiana che istituisce un elenco di soggetti critici (ministeri, operatori rete, aziende difesa, ecc.) e prescrive per essi misure di sicurezza rafforzate. Prevede la notifica e il vaglio governativo per l'acquisto di tecnologie ICT da fornitori extra-UE, con possibile veto (Golden Power) se ritenute rischiose per la sicurezza nazionale. È un potente strumento di tutela dell'indipendenza tecnologica: grazie ad esso l'Italia ha potuto condizionare l'uso di apparecchiature cinesi nel 5G e in altre reti strategiche.
- Digital Services Act (DSA) – UE Reg. 2022/2065: entrato in vigore nel 2023, regola le grandi piattaforme online (social network, marketplace, motori di ricerca) imponendo obblighi per controllo dei contenuti illegali, trasparenza algoritmica, auditing e gestione dei rischi sistemici. Pur non riferendosi direttamente al grado di controllo sui dati nel territorio fisico del Paese, il DSA di fatto riafferma il potere normativo europeo sulle piattaforme digitali globali, costringendole ad adeguare i propri servizi alle regole decise dall'UE. L'Italia, attraverso AGCOM, è attiva nell'enforcement del DSA sui servizi operanti nel suo territorio.
- Digital Markets Act (DMA) – UE Reg. 2022/1925: in vigore da maggio 2023, mira a limitare gli abusi di potere di mercato dei "gatekeeper" digitali (Big Tech dominanti). Impone, ad esempio, l'obbligo per Apple e Google di aprire i propri app store ad alternative, di permettere interoperabilità tra piattaforme di messaggistica, ecc. Anche questa normativa aumenta l'autonomia europea, riducendo il rischio che le scelte tecnologiche di imprese e cittadini italiani siano *imposte* dalle policy di pochi attori stranieri.
- Data Governance Act (DGA) e Data Act – UE 2022/868 (DGA) e proposta 2022 (in approvazione per Data Act): il DGA istituisce regole per facilitare la condivisione di dati tra enti pubblici e privati in UE in modo volontario e controllato, anche tramite *altruismo dei dati* e provider di spazi di dati. Il Data Act invece fornirà un quadro su chi può accedere e utilizzare i dati generati da dispositivi IoT e servizi, con l'obiettivo di evitare concentrazione di dati in mani di pochi (come i produttori dei device) e dare opportunità ad attori europei. Insieme, queste norme creano un mercato dei dati equo, in cui i dati generati in Italia possano essere

sfruttati a beneficio dell'economia locale, e non estratti e portati all'estero senza ritorno.

- Chips Act europeo – Reg. 2023/1781: approvato nel 2023, mobilita 43 miliardi di euro (pubblici e privati) per sviluppare l'industria dei semiconduttori in Europa. Include un meccanismo di coordinamento in caso di crisi nella supply chain e fondi per nuovi impianti (come quello di STM a Catania finanziato dal Governo). Per l'Italia significa poter sostenere con aiuti di Stato la crescita di proprie fabbriche e centri R&D microelettronici, cosa altrimenti proibita dalle norme sugli aiuti UE. È dunque un abilitatore chiave per recuperare indipendenza nella filiera chip.
- AI Act (in fase di finalizzazione nel 2024): la futura regolamentazione europea sull'intelligenza artificiale imporrà requisiti di trasparenza, valutazione di conformità e divieti per sistemi di AI considerati ad alto rischio (es. riconoscimento facciale massivo). Garantirà che l'uso dell'AI in Italia avvenga secondo i valori europei e ridurrà la dipendenza da algoritmi "black box" sviluppati all'estero, imponendo ad esempio la documentazione dei modelli e la possibilità di auditing su di essi.

- Norme nazionali sulla trasformazione digitale: infine, a livello italiano vi sono direttive e linee guida emanate da AgID e dal Dipartimento per la Trasformazione Digitale che indirizzano le PA verso tecnologie sicure e interoperabili (ad es. obbligo del cloud first, utilizzo di API aperte, adesione a PagoPA, SPID/CIE per identità digitale, ecc.). Citate in precedenza, ricordiamo la Determina AgID 628/2021 sul Cloud e il nuovo Regolamento unico di ACN per le infrastrutture e i servizi cloud per la PA, le Linee guida su acquisizione e riuso di software, e il Piano Triennale per l'Informatica nella PA. Anche se non leggi in senso stretto, questi atti amministrativi concorrono a costruire un ecosistema digitale più autonomo, evitando frammentazione e dipendenze duplicative (un esempio: l'adesione universale a SPID/CIE riduce la necessità per i cittadini di usare credenziali social media – Google, Facebook – per accedere ai servizi pubblici, mantenendo l'identità digitale sotto controllo nazionale).

In sintesi, l'arsenale normativo a disposizione dell'Italia e dell'Europa è ampio e in continuo aggiornamento. Esso costituisce la cassetta degli attrezzi con cui difendere e accrescere la propria indipendenza digitale: dal controllo delle infrastrutture critiche (NIS2, perimetro cyber) alla regolazione delle piattaforme globali (DSA/DMA), dalla protezione dei dati (GDPR) al sostegno industriale (Chips Act). Il corretto recepimento e

l'effettiva applicazione di queste norme saranno determinanti per tradurre la legge in risultati tangibili sul campo digitale.

Il ruolo di enti pubblici e privati nella transizione digitale e verso l'indipendenza tecnologica

Il cammino verso una maggiore indipendenza digitale coinvolge una molteplicità di attori. In Italia, sia enti pubblici dedicati sia aziende private svolgono ruoli complementari nel promuovere la transizione digitale e garantire la indipendenza tecnologica.

Gli attori pubblici istituzionali

- **Dipartimento per la Trasformazione Digitale (DTD)**: struttura di coordinamento presso la Presidenza del Consiglio (già Ministero dell'Innovazione), responsabile dell'attuazione dell'Agenda Digitale italiana e dei progetti PNRR sul digitale. Il DTD ha elaborato strategie chiave come quella sul Cloud, guida il piano "Italia Digitale 2026" e supervisiona l'implementazione di SPID, PagoPA, app IO, IT Wallet etc. Il suo ruolo è garantire che la digitalizzazione della PA avvenga in modo coerente e **in linea con gli obiettivi di autonomia** (ad esempio, promuovendo standard aperti e sicurezza by design).
- **Agenzia per l'Italia Digitale (AgID)**: ente tecnico che definisce regole e qualificazioni su ICT nella PA. AgID monitora l'adozione del **Piano Triennale ICT**. Inoltre, AgID supporta i progetti di open source e interoperabilità (cataloghi di API, dati, software) contribuendo a un ecosistema digitale più **aperto e controllabile localmente**.

- **Agenzia per la Cybersicurezza Nazionale (ACN)**: come già descritto, è l'architrave della resilienza cybernetica italiana. Coordina le difese cyber, emette indicazioni tecniche vincolanti per gli enti nel Perimetro di sicurezza, gestisce gli incidenti e rappresenta l'Italia nei consessi UE sulla cybersecurity. L'ACN è anche investita di compiti di **sviluppo industriale**: agendo come Centro di coordinamento del Competence Centre UE, eroga fondi per progetti di ricerca cyber domestici.

- **Cassa Depositi e Prestiti (CDP)**: braccio finanziario del governo, ha assunto un ruolo attivo nel settore digitale come investitore strategico. CDP (tramite la controllata CDP Equity) detiene il 60% di Open Fiber (società che posa fibra FTTH) e ha quote in vari progetti: 20% nel PSN,

partecipazioni in TIM (fino al 10% prima di recenti riassetti) e in alcune startup tech tramite il Fondo Nazionale Innovazione. L'obiettivo di CDP è sostenere infrastrutture e aziende considerate di interesse nazionale, mantenendone la proprietà in mani italiane.

- **Altri enti pubblici**: il Ministero delle Imprese e del Made in Italy (MIMIT) gestisce dossier come il **5G e Golden Power** su forniture TLC; il Ministero della Difesa tramite il CIOC (Comando Interforze Operazioni Cibernetiche) sviluppa capacità offensive/difensive cyber; il Garante Privacy vigila sul rispetto dei dati personali; Banca d'Italia e CONSOB regolano aspetti cyber nel settore finanziario. Tutti collaborano nell'**Architettura Nazionale Cyber** definita dal DPCM 2022, dove ACN è cabina di regia. Questa rete istituzionale integrata è una garanzia che la transizione digitale avvenga con attenzione alla **cybersicurezza e alla indipendenza in ogni ambito.**

Il ruolo del settore privato nazionale

- **Operatori di telecomunicazioni**: forniscono l'infrastruttura di connettività aziende come **TIM**, **Open Fiber**, **Fastweb+Vodafone**, **WindTre**, **Iliad** e una costellazione di operatori indipendenti attivi da oltre 25 anni, che hanno portato la connettività in aree industriali, rurali e periferiche dove i grandi operatori non sono mai arrivati. Questi operatori, molti dei quali aderenti ad **AIIP**, sono stati pionieri nella posa di fibra ottica, nella realizzazione di dorsali diversificate e nello sviluppo di datacenter edge ad altissima efficienza, oltre ad aver creato i principali IXP Italiani.

TIM in particolare, storico ex-incumbent, oltre a gestire una parte della rete fissa, ha presenza, con **TIM Enterprise**, nel cloud (Noovle) e cybersecurity (Telsy) e – con recente ritorno sotto controllo italiano tramite Poste Italiane– viene vista come un asset strategico per la **indipendenza digitale del Paese**). Un controllo nazionale di TIM ridurrebbe i rischi di dipendenza da operatori esteri e garantirebbe che le reti critiche restino sotto governance italiana. Open Fiber, partecipata dallo Stato, sta cablando aree dove il mercato non arriva, assicurando parità territoriale nell'accesso a internet. In prospettiva, la **fusione rete Fibercop-OF** creerebbe un campione nazionale delle telecomunicazioni. È importante notare che anche gli operatori mobili stranieri (Iliad, Fastweb+Vodafone) devono rispettare le regole italiane e sottostanno al Golden Power: ciò mantiene comunque la **supremazia decisionale italiana** su elementi sensibili (ad es.,

nel 2023 Iliad ha dovuto escludere fornitori cinesi dall'accesso core su indicazione governativa).

- **Fornitori cloud italiani**: **come Aruba, promuovono un'offerta cloud italiana e quindi europea. Queste aziende evidenziano come, per motivi di cybersecurity e protezione dati, sia fondamentale valorizzare i provider italiani. La presenza di cloud provider domestici offre anche benefici economici (sviluppo di filiera locale, posti di lavoro qualificati) e garantisce che in caso di tensioni geopolitiche l'Italia non si trovi senza risorse cloud. Alcune grandi imprese ICT nazionali sono anch'esse attive: Leonardo ha una divisione cyber & cloud che, oltre a partecipare al PSN, fornisce servizi cloud privati e sicurezza avanzata a Ministeri e aziende; Fincantieri (difesa) e Ferrovie (infrastrutture) stanno creando cloud dedicati per i propri settori con partner italiani. Anche ENEA e CINECA contribuiscono con infrastrutture di ricerca (HPC e cloud scientifici) aperte a comunità italiane.**

- **Industria tecnologica e manifatturiera**: aziende come **STMicroelectronics** (microchip), **Olivetti** (società del Gruppo TIM specializzata nell'IoT, che opera nell'ambito di TIM Enterprise), **Exprivia** (software), **Soluzioni PA** (gestionali PA) e molte PMI innovative svolgono un ruolo nella produzione di tecnologia "made in Italy". La loro competitività sul mercato globale è sostenuta da iniziative statali (credito d'imposta R&S, bandi PNRR) che mirano a creare campioni nazionali in settori strategici. Un esempio di successo è **Olivetti** – marchio storico italiano – realtà rinnovata e in evoluzione, la Digital Company di TIM che sviluppa soluzioni negli ambiti dell'Internet of Things, dell'AI e dei Big Data, per settori come le Smart City e Smart Industry con un posizionamento distintivo nell'abilitazione del business attraverso l'innovazione digitale sfruttando, in particolare, la tecnologia 5G.

- **Academia e centri di ricerca**: le università e i centri pubblici (CNR, IIT, ENEA, ecc.) sono parte del tessuto che assicura competenze domestiche. Programmi come **National Centre on HPC, Big Data and Quantum Computing** (finanziato dal PNRR, con hub a Bologna) o il **Centro Nazionale Cybersecurity** (CINI Cybersecurity National Lab) riuniscono decine di

atenei e industrie per sviluppare tecnologie avanzate localmente. L'obiettivo è duplice: formare **professionisti altamente specializzati** (riducendo la dipendenza da know-how esterno) e creare prototipi/soluzioni che possano essere industrializzati in Italia. Ad esempio, nel campo dei microprocessori, il Politecnico di Milano e di Torino partecipano a progetti UE su architetture RISC-V e fotonica integrata, così che un domani l'Italia possa avere proprietà intellettuale in componenti critici.

In conclusione, la collaborazione pubblico-privato è fondamentale: le istituzioni fissano la rotta e finanziano infrastrutture, mentre le aziende implementano le soluzioni e innovano. Allineare gli interessi (ad esempio coinvolgendo le aziende nazionali nei grandi progetti PA) è la chiave affinché la transizione digitale italiana sia anche un'occasione di rafforzamento dell'industria locale. Quando un servizio digitale strategico può essere fornito da un soggetto italiano o europeo, è auspicabile che ciò avvenga, pur mantenendo un sano livello di concorrenza. In caso contrario, laddove si usi un fornitore estero, il ruolo del pubblico è mitigarne i rischi tramite contratti e controlli (come sta avvenendo con l'accordo di interoperabilità per i dati sanitari con piattaforme cloud estere soggette a stretti vincoli GDPR). L'ecosistema italiano sembra aver compreso questa filosofia e sempre più spesso si osservano partnership "di sistema" (es. TIM con Google Cloud sotto governance italiana, Leonardo con Microsoft per Azure in PSN, ecc.) volte a coniugare migliori tecnologie globali con la tutela degli interessi nazionali.

Il confronto con gli altri Paesi Europei sul fronte dell'indipendenza digitale

La spinta verso l'indipendenza digitale non è una peculiarità italiana, ma un trend europeo. Tuttavia, diversi Paesi hanno approcci e livelli di avanzamento differenti. Confrontare l'Italia con altre nazioni UE aiuta a contestualizzare punti di forza e lacune.

La **Francia** si distingue come una delle nazioni più attive nel perseguire l'autonomia tecnologica, un impegno evidenziato dall'adozione, a partire

dal 2019, di una strategia nazionale denominata "cloud di fiducia"; questa iniziativa mira a certificare i fornitori di servizi cloud che soddisfano requisiti specifici per la gestione dei dati pubblici sensibili, garantendo così maggiore sicurezza e controllo. Parallelamente, il governo francese ha energicamente promosso la creazione e l'adozione di soluzioni cloud nazionali, come dimostra la nascita di una joint venture strategica tra due aziende francesi che utilizza tecnologia Microsoft ma opera sotto un rigoroso controllo francese, e l'accordo tra un'azienda francese e Google volto a fornire servizi cloud conformi alla dottrina di indipendenza francese, assicurando che i dati siano criptati e accessibili esclusivamente da entità francesi. Oltre al settore cloud, la Francia investe cospicue risorse nella cyberdifesa, vantando uno dei budget più elevati dedicati alla cybersicurezza all'interno dell'Unione Europea. Sul piano normativo, la Francia si è dimostrata pioniera nell'introdurre misure come la tassa sui servizi digitali e nell'esercitare pressioni antitrust nei confronti delle grandi aziende tecnologiche globali (Big Tech). Questo approccio proattivo e multidimensionale ha prodotto risultati concreti: oggi le pubbliche amministrazioni francesi possono contare su un ampio ventaglio di soluzioni cloud domestiche certificate e il paese si posiziona come sede di progetti tecnologici all'avanguardia, come testimonia l'imminente installazione in Francia di "Jupiter", il secondo supercomputer exascale europeo. Nel confronto, l'Italia sta compiendo sforzi per recuperare terreno seguendo un modello simile, ad esempio attraverso l'implementazione del Polo Strategico Nazionale (PSN) e la promozione di collaborazioni industriali analoghe, come quella tra Leonardo e Defence Tech per lo sviluppo di un cloud sicuro, sebbene parta da una posizione di maggiore svantaggio iniziale rispetto all'avanzamento francese.

La **Germania** ha attraversato una significativa transizione nella sua politica relativa all'infrastruttura digitale e alla indipendenza tecnologica. Se inizialmente la Pubblica Amministrazione tedesca adottava un approccio relativamente aperto verso il mercato cloud, con limitate restrizioni nella selezione dei fornitori, negli anni recenti si è verificato un sostanziale riorientamento strategico. Questo cambiamento si è concretizzato in due principali iniziative: l'assunzione di un ruolo di co-leadership nel progetto paneuropeo Gaia-X e l'implementazione di linee guida che privilegiano fornitori cloud europei per settori considerati critici per la sicurezza nazionale. Un elemento distintivo del panorama tecnologico tedesco è la presenza di solidi attori industriali autoctoni che contribuiscono significativamente alla resilienza digitale del paese: SAP, leader mondiale

nel software enterprise; Siemens, protagonista nell'industria 4.0 e nelle tecnologie per l'automazione industriale; Deutsche Telekom, che attraverso la sua divisione T-Systems offre servizi cloud e IT, con iniziative emergenti come "Open Telekom Cloud", orientate verso architetture federate; e Infineon, azienda europea di primaria importanza nel settore dei semiconduttori. Questa costellazione di attori nazionali conferisce alla Germania una relativa autonomia in determinati segmenti tecnologici. Ad esempio, una porzione significativa di dati industriali tedeschi risiede su infrastrutture cloud SAP localizzate in territorio nazionale, limitando la dipendenza da fornitori extra-europei. Nonostante i punti di forza evidenziati, la Germania condivide con l'Italia alcune carenze infrastrutturali significative. In particolare, la connettività in fibra ottica nel territorio tedesco presenta tassi di penetrazione inferiori persino a quelli italiani: nel 2022, la penetrazione FTTH (Fiber To The Home) in Germania si attestava al 10%, contro il 16% dell'Italia. Solo recentemente le autorità tedesche hanno avviato programmi di accelerazione in questo ambito. La struttura economica tedesca, fortemente orientata all'export, influenza in modo determinante le politiche digitali del paese. Berlino tende ad adottare un approccio cauto verso misure che potrebbero innescare ritorsioni commerciali da parte dei partner internazionali. Questo spiega, ad esempio, la maggiore prudenza rispetto alla Francia nell'implementare restrizioni verso fornitori come Huawei. Germania e Italia rappresentano partner strategici nel contesto europeo per quanto concerne le politiche digitali, con posizioni allineate su diverse questioni: entrambi i paesi sostengono attivamente l'allocazione di fondi europei per lo sviluppo della microelettronica, condividono l'interesse per la definizione di standard comuni per cloud computing e intelligenza artificiale, mantengono solide collaborazioni nell'ambito della ricerca scientifica, con iniziative congiunte nel quantum computing, e presentano potenzialità di cooperazione nel cloud industriale, con possibili sviluppi verso soluzioni federate che interconnettano i rispettivi distretti manifatturieri. Un elemento distintivo del contesto tedesco è rappresentato dalla struttura federale dello stato, che conferisce ai singoli Länder un'ampia autonomia nella definizione delle proprie strategie digitali. Questa configurazione comporta sfide di coordinamento più complesse rispetto al modello italiano, caratterizzato da un maggiore centralismo amministrativo. In conclusione, sebbene Germania e Italia presentino differenze significative nell'ecosistema tecnologico e nelle strutture di governance, entrambe le nazioni stanno convergendo verso una visione strategica della indipendenza digitale che

privilegia la cooperazione europea, pur mantenendo specifiche peculiarità nazionali che riflettono i rispettivi contesti industriali e istituzionali.

La **Spagna** rappresenta un caso di studio particolarmente interessante nel panorama europeo della digitalizzazione, avendo adottato una strategia che integra efficacemente investimenti in infrastrutture di connettività e sviluppo di servizi pubblici digitali avanzati. Questo approccio ha prodotto risultati considerevoli, collocando il paese in una posizione di leadership continentale per quanto concerne la penetrazione della fibra ottica, con oltre il 78% delle famiglie connesse mediante tecnologia FTTH (Fiber To The Home), un dato significativamente superiore alla media europea. Parallelamente, la Spagna ha compiuto progressi sostanziali nel dominio dell'open data, implementando sistemi che favoriscono la trasparenza e l'accessibilità delle informazioni pubbliche. In materia di indipendenza digitale, l'approccio spagnolo si caratterizza per un pragmatismo strategico che bilancia l'apertura agli investimenti internazionali con la tutela degli interessi nazionali. Questa impostazione ha consentito al paese di attrarre importanti investimenti infrastrutturali da parte dei principali attori tecnologici globali: Google ha selezionato la Spagna come sede per l'installazione di una Cloud Region e per l'approdo di cavi sottomarini transatlantici, e analoghe decisioni sono state adottate da Microsoft. Contestualmente, il governo spagnolo sta sviluppando il progetto GAIA-X Iberico in collaborazione con il Portogallo, cercando di stabilire un equilibrio funzionale tra la presenza di operatori internazionali e il mantenimento di un adeguato controllo locale sulle infrastrutture critiche.

A differenza dell'Italia, la Spagna non ha istituito un equivalente del Polo Strategico Nazionale (PSN), optando invece per un sistema basato su contratti quadro per l'acquisizione di servizi cloud destinati alla Pubblica Amministrazione, con un ventaglio di fornitori certificati secondo specifici parametri di sicurezza e affidabilità. Nel campo della cybersecurity, la Spagna manifesta un elevato livello di proattività: l'Instituto Nacional de Ciberseguridad (INCIBE) opera con efficacia come agenzia nazionale di riferimento, e si registra una collaborazione particolarmente virtuosa tra settore civile e militare nella gestione delle minacce informatiche. La Spagna si configura pertanto simultaneamente come un concorrente e come un modello di riferimento per l'Italia in diverse dimensioni della trasformazione digitale. Particolarmente significativa è la capacità dimostrata dal paese iberico nel recuperare più celermente il divario digitale relativamente all'infrastruttura in fibra ottica. Entrambe le nazioni

condividono l'obiettivo strategico di evitare una posizione di subalternità nell'ecosistema digitale europeo e globale; tuttavia, disponendo di risorse più limitate rispetto a Francia e Germania, si trovano frequentemente nella necessità di consolidare le proprie forze mediante iniziative congiunte. Un esempio emblematico di questa cooperazione è rappresentato dall'alleanza europea sui dati turistici, un progetto coordinato congiuntamente da Italia e Spagna che mira a valorizzare un settore economico fondamentale per entrambi i paesi attraverso la gestione strategica dei dati correlati.

I **paesi nordici** presentano un approccio distintivo alla indipendenza digitale, caratterizzato da un equilibrio tra apertura globale e protezione degli interessi nazionali. Riportiamo di seguito alcuni cenni.

L'**Estonia**, considerata pioniere nell'e-Government, ha sviluppato un sistema di governo digitale resiliente basato su una rete distribuita di data center nazionali. Il programma e-Estonia include l'innovativo concetto di "data embassy", con server situati anche in Lussemburgo per garantire la continuità dei servizi essenziali in caso di crisi. L'Estonia utilizza la tecnologia blockchain per l'integrità dei registri pubblici e ha implementato il sistema X-Road per l'interoperabilità sicura tra servizi pubblici e privati.

La **Finlandia** ha investito significativamente nella propria resilienza digitale pur rimanendo aperta ai servizi globali. Il Finnish Digital Agency coordina lo sviluppo di servizi digitali nazionali, mentre la strategia di cybersicurezza nazionale prevede collaborazioni pubblico-private per proteggere infrastrutture critiche. La Finlandia ha inoltre creato il Finnish Center for Artificial Intelligence (FCAI) per sviluppare competenze nazionali in intelligenza artificiale.

La **Danimarca** basa la sua strategia su un forte quadro normativo e sulla promozione dell'alfabetizzazione digitale. L'Agency for Digital Government (Digitaliseringsstyrelsen) supervisiona l'implementazione di soluzioni digitali pubbliche, mentre il Danish Centre for Cyber Security

fornisce protezione contro le minacce informatiche. La Danimarca ha implementato NemID/MitID come sistema di identità digitale nazionale e mantiene strette collaborazioni con altri paesi nordici per lo sviluppo di standard interoperabili.

La **Polonia** sta emergendo come attore significativo nel panorama digitale europeo. Il progetto "Chmura Krajowa" (National Cloud) rappresenta una collaborazione strategica tra il governo polacco, il banco PKO BP e partner tecnologici globali come Google e Microsoft. L'iniziativa prevede la creazione di infrastrutture cloud localizzate sul territorio nazionale ma gestite con tecnologie internazionali, sotto il controllo di operatori polacchi. La Polonia ha inoltre lanciato il programma "PolFEOR" (Polish Future and Emerging Technologies Development Program) per sviluppare capacità tecnologiche nazionali in settori strategici come intelligenza artificiale, blockchain e quantum computing.

La **Repubblica Ceca** ha adottato la strategia "Digital Czech Republic", che include progetti per rafforzare l'indipendenza digitale del paese. L'iniziativa comprende lo sviluppo di un'infrastruttura cloud governativa nazionale, investimenti in cybersicurezza e lo sviluppo di competenze digitali. La Repubblica Ceca ha inoltre istituito il National Agency for Communication and Information Technology (NAKIT) per coordinare gli sforzi governativi in ambito digitale (Government of the Czech Republic, 2023).

Le conclusioni e le prospettive future

Dal quadro emerso, l'Italia ha intrapreso un percorso deciso verso una maggiore indipendenza digitale, pur essendo ancora in una fase di transizione. Allo stesso tempo, l'Italia resta parte di un contesto europeo dove l'indipendenza digitale si costruisce collettivamente: il successo di molte delle iniziative esaminate (il Chips Act o la Bussola Digitale 2030) potrà essere determinante per tutti i membri UE.

In prospettiva, l'Italia dovrà continuare a equilibrare apertura e autonomia. Ciò significa, da un lato, continuare a innovare e integrarsi nelle catene globali (per non perdere competitività) e dall'altro lato le sarà chiesto di dotarsi dei necessari piani di emergenza con salvagenti locali, per ogni catena di tecnologie considerata strategica. Il concetto di *"autonomia strategica aperta"* dell'UE sintetizza bene questo approccio: cooperare con alleati e utilizzare le migliori tecnologie disponibili, ma mantenendo la capacità di agire in modo autonomo quando necessario.

In definitiva, l'indipendenza digitale non è un traguardo assoluto da conseguire una volta per tutte, ma un processo continuo di adattamento e rafforzamento. L'obiettivo realistico per l'Italia non è tanto l'autarchia tecnologica (velleitaria e ormai operativamente impraticabile) quanto la capacità di scelta autonoma: poter decidere quali tecnologie adottare e da chi acquisirle in base al proprio interesse nazionale e non per mancanza di alternative, nella consapevolezza degli eventuali rischi. Questo approccio non può prescindere dal valorizzare il contributo degli operatori territoriali che, da anni, rappresentano l'avanguardia tecnica del Paese, dimostrando nei fatti che è possibile coniugare autonomia infrastrutturale, innovazione e presidio locale delle reti e dei dati.

I passi compiuti finora – dalla banda ultralarga alle nuove norme, fino al cloud nazionale – indicano la direzione giusta, ma non è sufficiente e le strategie necessarie saranno esaminate nel libro bianco.

Il Libro Bianco

Il **Libro Bianco** che nel corso dell'anno accompagnerà l'uscita di questo Rapporto si configura come un documento strategico di ampio respiro, orientato a fornire un quadro analitico e propositivo sulle condizioni necessarie per garantire **l'indipendenza digitale** di un ecosistema nazionale o sovranazionale, nel contesto dell'interdipendenza globale delle tecnologie critiche.

Le analisi delle tecnologie critiche e delle supply chain

In apertura, il documento offrirà un'**analisi approfondita delle tecnologie considerate critiche**: le infrastrutture digitali, i sistemi operativi, i chip e le tecnologie di comunicazione (come le reti 5G/6G e satellitari). Saranno esaminate le **catene di fornitura**, con l'obiettivo di individuare vulnerabilità strutturali e **leve strategiche** per rafforzare il controllo e la governance. Tale approccio implica l'adozione di una prospettiva tecno-economica, in cui le norme assumono un valore regolativo sulla tecnica, ma anche la responsabilità di modificarne la struttura in funzione di valori condivisi.

I casi di studio e governance multilivello

Il documento sarà arricchito da **casi di studio forniti dalle imprese** partecipanti all'iniziativa, trasformati in osservazioni critiche e riflessioni propositive. Questi illustreranno esperienze di implementazione tecnologica e di transizione digitale, contribuendo a una visione articolata delle esigenze di governance. Sarà essenziale evitare una mera reiterazione delle esperienze: occorre piuttosto fare emergere **pattern normativi** e criticità ricorrenti, in modo da proporre modelli replicabili.

Saranno inoltre inclusi **esempi internazionali**, tra cui il caso Eurostack, che fornisce un modello esemplare di costruzione di indipendenza digitale attraverso standard comuni, investimenti in infrastrutture condivise e normative coordinate. Tali riferimenti offriranno un confronto utile per evidenziare le **diverse filosofie normative** adottate nei contesti globali (es. approccio libertario vs. approccio paternalista nella regolazione delle reti e della privacy).

Le raccomandazioni operative e roadmap

Il Libro Bianco intende raccogliere una **serie di raccomandazioni operative**, dirette ai decisori politici, alle imprese, alla società civile e alle istituzioni. Tali raccomandazioni costituiranno le basi per costruire una **roadmap concreta verso un ecosistema digitale più sicuro, resiliente e libero, almeno in prospettiva, da condizionamenti esterni**. In tal senso, saranno articolati percorsi normativi che si ispirano a una **semantica del diritto positiva e performativa**, in cui la norma non solo descrive ma modifica lo stato di cose (cfr. Lessig, *Code*, e Rossetti, *Dare regole alle nuove tecnologie*).

Le dimensioni dell'Indipendenza Digitale

L'indipendenza digitale potrebbe essere misurata attraverso una valutazione multilivello del grado di controllo, autonomia e consapevolezza rispetto a infrastrutture, tecnologie e servizi digitali considerati essenziali per l'interesse collettivo. Gli impatti da analizzare per evidenziare le potenziali aree di rischio, quindi, possono essere affrontati da tre diverse prospettive: dal punto di vista governativo, da quello organizzativo (pubblico o privato) e dal punto di vista dei cittadini.

La prospettiva dei Governi (UE e Italia)

I governi hanno la responsabilità strategica di definire regole, standard e architetture che garantiscano le caratteristiche dell'indipendenza digitale. I gradi di indipendenza possono infatti dipendere da:

- la capacità di pianificare infrastrutture digitali autonome;
- la "forza" (fatta di consapevolezza e competenze) di riuscire a incentivare software pubblici open e sicuri;
- l'orientamento culturale alla promozione di standard aperti e interoperabili;
- la presenza di strumenti per la protezione dei dati e la sicurezza nazionale.

La prospettiva delle Organizzazioni (Enti pubblici e imprese)

Per le organizzazioni, l'indipendenza digitale consiste nella possibilità di scegliere, adattare e integrare tecnologie in modo conforme a esigenze interne e normative, con l'intento ultimo di:

- evitare lock-in tecnologici;
- valorizzare e presidiare soluzioni software strategiche (es. ERP, CRM, PEC...);
- garantire la sicurezza e la continuità operativa;
- contribuire attivamente alla costruzione di ecosistemi interoperabili (o a non allestire barriere all'interoperabilità).

La prospettiva dei Cittadini

Per i cittadini, l'indipendenza digitale è accesso equo, sicuro e trasparente, possibilmente sempre disponibile, ai servizi digitali essenziali, con garanzie su:

- protezione dei propri dati;
- possibilità di accedere ad ambienti digitali affidabili;
- possibilità di gestire con flessibilità e continuità i propri diritti in ambito digitale;
- disporre di competenze digitali sufficienti per un uso autonomo delle tecnologie.

I principali assi decisionali per l'indipendenza digitale

Per parlare concretamente di indipendenza digitale, è necessario partire dall'identificazione di alcune aree strategiche, su cui prendere decisioni, orientando politiche pubbliche, investimenti e azioni concrete.

L'indipendenza digitale è un principio trasversale che incide sulla qualità della vita, sulla sicurezza e sulla tutela dei diritti, sulla capacità di disporre di autonomia, se necessario, e sulla possibilità di crescere in innovazione in modo stabile e sostenibile. È anche, come abbiamo visto, uno strumento di prevenzione rispetto a forme più o meno conosciute e consapevoli di dipendenza o opportunismo, che possono impattare nell'erogazione e nella fruizione di tecnologie e servizi (digitali) alla popolazione.

In questo quadro, si possono identificare quattro principali direttrici tecniche portanti, assi decisionali su cui costruire percorsi di autonomia digitale consapevole: infrastrutture (la cui fruizione dovrebbe avvenire in garanzia di continuità), sicurezza e protezione (la cui tutela e salvaguardia dovrebbe essere un diritto prioritario), applicativi sensibili (la cui indipendenza da rischi di discontinuità dovrebbe essere indispensabile) e interoperabilità (la cui presenza abbatte costi di switching e univocità di servizio).

Le Infrastrutture digitali e la connettività

Le reti di connessione (fisica, satellitare, ecc.), i servizi in cloud (storage, microservizi, accessibilità, salvaguardia, ecc.), i data center e le architetture edge rappresentano la base su cui poggia ogni tipo di servizio digitale. L'indipendenza su questo fronte richiede che queste infrastrutture siano continuativamente accessibili, localizzate e pertanto governabili, trasparenti e affidabili nella gestione dei dati. Come arrivare a questa condizione?

La sicurezza informatica e la protezione dei dati

Dimensione critica e trasversale, che comprende la stabilità dei sistemi informativi, la governance dei dati sensibili e la capacità di prevenire e gestire minacce digitali in continuo mutamento ed evoluzione. È il presupposto per garantire fiducia, continuità, legalità e capacità di difesa nell'ecosistema digitale. Quali decisioni prendere per rinforzare queste barriere?

I software sensibili di servizio pubblico

Sono tutti quei software indispensabili alla funzionalità della Pubblica Amministrazione e all'erogazione continuativa di servizi essenziali come Sanità, Istruzione, Identità Digitale, Giustizia ecc. In un ecosistema digitale, sono asset sostanziali per tutelare i diritti fondamentali di ogni individuo (diritti civili, economici, sociali, culturali, di pace, di lavoro, di sviluppo, ecc.). L'indipendenza si realizza attraverso mappe applicative conosciute, stabili e protette, potenzialmente soggette a controllo pubblico. In quali direzioni è corretto muovere per ottenere questo risultato?

Lo sviluppo di standard e soluzioni interoperabili

Per evitare frammentazione, lock-in tecnologici e rimanere intrappolati in contesti insostituibili, è necessario promuovere, sostenere e forse imporre standard aperti, condivisi e sostenibili, in grado di garantire l'interoperabilità tra sistemi, anche eterogenei, la scalabilità delle soluzioni e incidere in questa direzione sull'evoluzione dell'ecosistema digitale. Quali scelte è necessario fare e a quale livello, per affrontare questa problematica?

Queste quattro direttrici non sono perimetri chiusi quanto piuttosto elementi tra loro fortemente interconnessi che, nel loro insieme, determinano il grado di indipendenza digitale raggiungibile da una comunità, sia a livello di singolo Stato che di Unione. Affrontarne l'evoluzione con

consapevolezza rappresenta un insieme di sfide complesse che richiedono competenze, presidio e investimenti.

Le aree principali di impatto

Da diverse prospettive è quindi possibile prendere decisioni specifiche che sono in grado di influenzare il grado di indipendenza digitale che ci caratterizza. Le aree di impatto non sono tra loro isolate, ma subiscono l'incidenza di numerosi aspetti della società. Comprendere dove e come queste le nostre decisioni possono impattare è essenziale dal punto di vista politico, economico e sociale. Tra le principali aree di impatto si possono individuare le seguenti.

- **Salute** - la digitalizzazione dei sistemi sanitari migliora l'accesso e l'efficienza dei servizi, ma pone sfide importanti in termini di protezione dei dati sensibili e interoperabilità delle piattaforme.
- **Formazione** - l'indipendenza tecnologica influisce sulla qualità e sull'equità e l'indirizzo dell'istruzione digitale, un risultato che si può conseguire favorendo la diffusione di competenze digitali – non necessariamente tecnologiche - di base e avanzate.
- **Sostenibilità** - un uso consapevole delle tecnologie può contribuire alla riduzione dell'impatto ambientale, grazie a infrastrutture energeticamente efficienti e a strategie di digitalizzazione sostenibile.
- **Giustizia** - la digitalizzazione del sistema giudiziario, se ben governata, può aumentare trasparenza, velocità e accessibilità ai procedimenti, rafforzando lo Stato di diritto.
- **Sicurezza** - la protezione dei sistemi informativi e dei dati è un presupposto fondamentale per garantire la sicurezza collettiva, prevenire minacce e gestire efficacemente eventuali situazioni di emergenza.
- **Lavoro** - l'indipendenza digitale consente di sviluppare strumenti adeguati per favorire il lavoro, la qualificazione professionale e il contributo a valore aggiunto della HI (human Intelligence), rafforzando così la competitività del sistema economico e imprenditoriale.
- **Economia** - una strategia digitale autonoma e coerente supporta la crescita di ecosistemi competitivi indipendenti da rischi di coercizione.
- **Innovazione** - promuovere tecnologie aperte, investire in ricerca indipendente e valorizzare il know-how interno sono condizioni essenziali per un'innovazione sostenibile e inclusiva, orientata a creare una diversa consapevolezza e nuove prospettive in ciascuno di noi.

L'obiettivo di questo elenco è quello di fotografare zone di influenza il più possibile marcate, nella piena consapevolezza che non solo l'elenco stesso è parziale ma è anche in continuo divenire.

L’indipendenza digitale, dunque, non si esaurisce nell’ambito tecnologico, ma si configura come un vero e proprio fattore abilitante per garantire nel tempo e a fronte di fenomeni turbolenti, uno stabile equilibrio collettivo. Affrontarne e prevenirne ogni possibile impatto può essere una sfida impossibile da affrontare, tuttavia siamo, tutti e ciascuno, chiamati a crescere in consapevolezza, per prevenire rischi e condividere regole di rispetto che vincolino la leva tecnologica nell’alveo delle opportunità, evitando gli opportunismi.