SICUREZZA DIGITALE E INDIPENDENZA: I PILASTRI DEL CLOUD SOVRANO

PIETRO LABRIOLA

Indice

Introduzione

Viviamo in un'epoca in cui i dati - così come gli algoritmi e le applicazioni - sono il nuovo petrolio[1]. Alimentano l'economia digitale, guidano le decisioni strategiche e definiscono il vantaggio competitivo delle nazioni. Ma, come il petrolio, i dati hanno bisogno di infrastrutture per essere verificati, raccolti, trasformati e distribuiti in sicurezza. Oggi queste infrastrutture si chiamano Cloud.

In un mondo interconnesso, la sovranità digitale è diventata una questione di sicurezza nazionale, di autonomia strategica e di competitività industriale. Non riguarda solo la Pubblica Amministrazione, riguarda l'intero sistema Paese.
Perché ogni giorno miliardi di informazioni sensibili attraversano reti e data center, spesso gestiti da operatori che rispondono a normative di Paesi terzi (extra EU). Questo espone le nostre imprese, le nostre istituzioni e i nostri concittadini a rischi concreti: cyberattacchi, spionaggio industriale, ingerenze giuridiche estere, violazioni di privacy e in ultima istanza rischio di dipendenza tecnologica e perdita di competitività dell'industria europea.

Il Cloud Sovrano è la risposta a questa sfida: un'infrastruttura digitale che garantisce che i dati, gli algoritmi e i servizi più importanti restino sotto il pieno controllo giuridico, tecnologico e operativo del Paese.

In Italia, il Polo Strategico Nazionale (PSN) rappresenta un primo passo concreto in questa direzione, ma la posta in gioco è più ampia: costruire un modello capace di proteggere e valorizzare l'intero ecosistema economico e sociale, pubblico e privato.

Questo instant book nasce con un obiettivo didattico: spiegare cos'è il Cloud Sovrano, perché è strategico, quali modelli esistono, quali benefici può portare e quali sfide comporta. Un percorso tra scenari internazionali, buone pratiche e visioni future, per capire perché oggi la sovranità digitale non è più un'opzione, ma una necessità.

Nell'economia digitale i dati sono la risorsa più strategica, alimento base dell'Intelligenza Artificiale. Come il petrolio nel secolo scorso, generano crescita, potere e innovazione. La differenza è che i dati non si esauriscono, ma si riutilizzano e si moltiplicano attraverso diversi servizi e applicazioni. L'Intelligenza Artificiale rende critici anche gli algoritmi che la implementano, oltre i dati stessi.

Come proteggere e governare questa risorsa in un mondo interconnesso ma geopoliticamente instabile? Vediamo di che si tratta.

[1] La frase "Data is the new oil" ("i dati sono il nuovo petrolio") è stata coniata dal matematico e imprenditore britannico Clive Humby nel 2006. Humby ha usato questa espressione per sottolineare che, come il petrolio grezzo, i dati grezzi di per sé non hanno valore se non vengono raffinati e analizzati per estrarne utilità e profitto.
Da allora, la frase è diventata molto popolare per evidenziare l'importanza strategica della capacità di elaborare i dati nell'economia digitale moderna.

Capitolo 1

I dati sono il nuovo petrolio.

Analizziamo il valore dei dati come risorsa strategica per economia, politica e innovazione.

Nel Novecento il petrolio ha dettato alleanze, conflitti e sviluppo industriale, nel XXI secolo il baricentro si è spostato su una nuova risorsa: oggi i dati rappresentano la leva strategica globale.
Ogni istante, miliardi di sensori, dispositivi e piattaforme producono un flusso ininterrotto di informazioni: una transazione bancaria, il tracciamento di una spedizione, un referto medico digitalizzato, un'interazione sui social. Tutto questo non è semplice "rumore digitale": è materia prima per decisioni economiche, sviluppo tecnologico, potere politico.
Ci sono tanti esempi della vita quotidiana che mostrano l'importanza dell'uso dei dati e come questi alimentano la crescita economica, il potere e l'innovazione.
Al supermercato, ogni volta che usiamo la carta fedeltà, possono essere raccolti i dati su cosa compriamo, quando e quanto spendiamo. Se il supermercato li usa bene, può offrirci sconti personalizzati, ottimizzare le scorte e non farci mai trovare il latte finito. Se lo fa è come avere un pozzo di petrolio, se non "estrae e raffina" resta solo terra.
Spotify e Netflix non ci conoscono di persona, ma sanno cosa ci piace ascoltare o guardare. Analizzano i nostri dati per creare playlist e suggerirci film che amerai. Senza quei dati, sarebbe come produrre carburante senza sapere per che tipo di motore.
In auto, ogni volta che usiamo Google Maps o Waze, inviamo informazioni sul nostro percorso e sulla velocità di guida. Insieme a milioni di altri utenti, quei dati permettono di segnalare incidenti e suggerire percorsi alternativi. È il carburante che tiene fluido il traffico digitale.
Nei match di Serie A o Champions League, sensori e telecamere raccolgono dati su ogni passaggio, tiro, corsa. Questi dati vengono analizzati per migliorare la preparazione atletica e le tattiche. È come trasformare il petrolio in carburante ad alte prestazioni per la squadra.
Usando i social network, ogni nostro like, commento o condivisione racconta qualcosa di noi. Le piattaforme usano questi dati per mostrarci contenuti mirati e inserzioni pubblicitarie personalizzate. È la loro benzina: senza, non girerebbe il motore del loro business.
Ma a differenza del petrolio, i dati non si esauriscono. Non si estraggono una volta sola per poi sparire, si moltiplicano in modo esponenziale, alimentati dalla crescente digitalizzazione della società e dell'economia. E il loro valore non risiede nel semplice possesso, ma nella capacità di raccolta, analisi, interpretazione e utilizzo.

Capitolo 2

Lo sviluppo del Cloud e i rischi attuali ed emergenti.

Ripercorriamo l'evoluzione del Cloud: nato come risposta a esigenze operative di riduzione dei costi e scalabilità, oggi è divenuto una vera infrastruttura strategica che abilita innovazione, gestione dei dati e competitività. Analizziamo come le imprese italiane affrontino il "Journey to Cloud" con strategie Multi Cloud e ibride, e come i dati, da semplice risorsa operativa, siano diventati un asset geopolitico e industriale. Mettiamo in luce anche i rischi legati alla perdita di controllo, ai conflitti di giurisdizione, al vendor lock-in e alle vulnerabilità tecnologiche, mostrando come il Cloud Sovrano emerga quale risposta necessaria per garantire sicurezza, resilienza e autonomia digitale.

Il Cloud nasce come risposta a bisogni operativi legati alla riduzione dei costi.
Negli anni '60-2000 gli obiettivi delle aziende si sono focalizzati sul risparmio dei costi hardware, sulla gestione dei picchi di domanda (scalabilità ed elasticità), sulla accessibilità di applicazioni e file ovunque (mobilità e collaborazione). Il Cloud nasce successivamente anche per dare una risposta a queste esigenze operative e infrastrutturali e oggi - nel moderno avanzamento del settore ICT - svolge un ruolo fondamentale come piattaforma primaria di erogazione dei servizi. La logica detta "Cloud First", cara a molti CIO e CEO delle aziende italiane, rappresenta l'opportunità di velocizzare i cicli ICT, di avere soluzioni scalabili e flessibili che abilitino il "Fail Fast", ossia la capacità di provare nuovi scenari e di riposizionare le risorse in caso di fallimento dell'iniziativa.
La conseguenza è che la maggioranza delle imprese del tessuto economico italiano ha un cosiddetto Journey to Cloud, ossia una strategia di esecuzione delle proprie applicazioni in Cloud. Non solo passano in Cloud le applicazioni aziendali, ma anche i servizi di base del moderno IT: sicurezza, autenticazione, protezione, backup, email, collaboration e in ultima istanza anche la connettività e parte della fonia. È un trend inarrestabile perché tutte le applicazioni sono sviluppate ormai in sola versione Cloud.
Il Journey to Cloud è arricchito da una strategia Multi Cloud con gestione ibrida[2]. Ciò si realizza quando un'organizzazione utilizza servizi di Cloud computing offerti da più fornitori, sia pubblici che privati, allo stesso tempo per ottimizzare prestazioni flessibilità e sicurezza. Si tratta di una strategia che inoltre riduce i rischi di vendor lock-in[3], interruzioni dovute a guasti o eventi estremi.
L'ulteriore evoluzione del Cloud è contrassegnata dal fatto che, quando si è concretizzata la possibilità di gestire grandi quantità di risorse in modo flessibile e condiviso, le aziende hanno iniziato a spostarvi sempre più dati e applicazioni. Questo ha creato ecosistemi di dati centralizzati, integrabili e sempre disponibili.
Oggi i dati non sono solo un "contenuto da archiviare", ma la vera risorsa strategica: alimentano AI, definiscono strategie, creano vantaggi competitivi. Senza il Cloud, questa valorizzazione dei dati su larga scala non sarebbe possibile: servono infatti infrastrutture elastiche, sicure e globali.

[2] Ci si riferisce ad un ambiente misto: parte delle risorse rimangono nei server aziendali, parte nel Cloud.
[3] Il vendor lock-in determina la difficoltà a migrare dati e applicazioni tra provider diversi.

In estrema sintesi, dal bisogno operativo (ottimizzare risorse) si è passati al bisogno strategico (trasformare i dati in innovazione). La conseguenza di questo straordinario fenomeno è la nascita di un vero e proprio mercato dei dati.
In numeri, il mercato globale dei dati valeva già circa 220 miliardi di dollari nel 2023 e crescerà di circa il 13% annuo nei prossimi anni[4].

Perché il Cloud è una infrastruttura strategica

Oggi il Cloud non è semplicemente "l'IT da un'altra parte": è il motore che alimenta la trasformazione digitale, l'innovazione tecnologica, la sicurezza dei dati e la resilienza delle infrastrutture critiche. Ma, se non governato, può diventare una leva di dipendenza tecnologica e industriale. Per questo motivo rappresenta un'infrastruttura strategica.
Infatti, i dati possono essere intercettati, copiati, manipolati o utilizzati in modi contrari agli interessi di chi li ha generati, mettendo a repentaglio servizi appartenenti a settori strategici come la sanità, la logistica, la finanza, l'energia, la Pubblica Amministrazione e, sempre più, le telecomunicazioni.
Inoltre, nell'attuale contesto geopolitico segnato da tensioni internazionali, conflitti, sanzioni economiche e cyberattacchi sempre più sofisticati, la localizzazione e la protezione delle informazioni diventano priorità di sicurezza nazionale.
Per tutelare l'infrastruttura strategica Cloud è essenziale mettere a fuoco i rischi che possono comprometterla.

Rischio di perdita di controllo sulla titolarità del dato

La perdita di controllo dei dati in contesti di Cloud o virtualizzazione comporta rischi di violazione della riservatezza, non conformità legale, perdita di disponibilità e limitata capacità di gestione e governance. In altre parole, quando un'organizzazione delega la custodia o l'elaborazione delle proprie informazioni a un fornitore esterno, si espone a una serie di vulnerabilità che non dipendono più direttamente dalle proprie politiche interne, ma dall'affidabilità, trasparenza del provider e, spesso, dalla normativa a cui quel provider è assoggettato.
Più in dettaglio, un primo ambito critico riguarda la sicurezza e la riservatezza. Ad esempio, un Cloud provider multi-tenant[5] può ospitare dati di più clienti sugli stessi server: se un attacco sfrutta una vulnerabilità dell'infrastruttura, l'accesso non autorizzato a dati sensibili di un'organizzazione diventa possibile. Inoltre, se la cifratura non è implementata correttamente, informazioni riservate come progetti di ricerca o cartelle sanitarie potrebbero essere intercettate durante la trasmissione.

[4] https://www.marketsandmarkets.com/Market-Reports/big-data-market-1068.html
[5] Il provider multi-tenant adotta un modello in cui più client (tenant) condividono la stessa infrastruttura e le stesse applicazioni mantenendo però dati e configurazioni separati e isolati.

Dal punto di vista legale e normativo, il problema principale è il possibile conflitto sulla giurisdizione del dato. Un'azienda europea che archivia informazioni personali in un data center situato negli Stati Uniti, ad esempio, potrebbe trovarsi soggetta al Cloud Act[6], che consente alle autorità americane di richiedere l'accesso ai dati, con il rischio di violare il GDPR. Inoltre, Il Cloud Act consente alle autorità statunitensi, tramite un mandato o una ingiunzione prevista dallo Stored Communications Act (SCA)[7], di richiedere dati a società americane anche se questi sono conservati all'estero. Questo crea conflitti di giurisdizione difficili da gestire e un'incertezza sulla reale protezione garantita agli interessati.

***Esempio**: la polizia scozzese e la Scottish Police Authority stanno adottando Office 365 per gestire dati personali e giudiziari. Recentemente Microsoft si è rifiutata di fornire alla polizia scozzese informazioni cruciali sui flussi internazionali dei dati caricati su Office 365, invocando la "riservatezza commerciale". Questa mancanza impedisce alle autorità di rispettare le norme del Data Protection Act 2018, che limita severamente il trasferimento di dati sensibili fuori dal Regno Unito[8].*

Il tema della giurisdizione del dato è strettamente correlato all'esigenza di vedere garantita la governance. Senza visibilità completa sui log e sulle modalità di trattamento, un'organizzazione non può verificare l'integrità delle informazioni né ricostruire con certezza eventuali anomalie[9].
A ciò si aggiunge un aspetto molto critico alla luce della attuale situazione geopolitica. I dati oggi cifrati con algoritmi classici (RSA, ECC, Diffie-Hellman) diventano vulnerabili ai computer quantistici futuri, che potranno violarli in tempi rapidissimi. Ciò riguarda non solo le comunicazioni correnti, ma anche archivi sensibili già conservati (sanità, finanza, difesa, infrastrutture critiche).
Il fenomeno di cui parliamo è noto come "harvest now, decrypt later": potenze straniere o attori malevoli possono intercettare e archiviare i dati oggi, per decifrarli quando la tecnologia quantistica sarà matura.
Le conseguenze sarebbero drammatiche: attacchi al settore pubblico, ad esempio tramite intercettazione delle comunicazioni diplomatiche e militari, comprometterebbero la sicurezza nazionale; attacchi al settore economico in generale determinerebbero l'accesso a proprietà intellettuale, brevetti, dati industriali che potrebbero es-

[6] "Clarifying Lawful Overseas Use of Data Act", del 23 marzo 2018.
[7] Legge federale statunitense del 1986, contenuta nel Titolo II dell'Electronic Communications Privacy Act (ECPA). Il suo scopo è regolare l'accesso delle autorità governative ai dati elettronici conservati da provider di comunicazioni.
[8] Computer Weekly .com, "Microsoft refuses to divuge data flows to Police Scotland", di Sebastian Kloving Skelton, 28 agosto 2025.
[9] I log sono registrazioni dettagliate delle operazioni che avvengono in un sistema informatico: accessi, errori, modifiche, tentativi di accesso non autorizzato, ecc. Ogni voce include informazioni importanti come timestamp, utente, componente coinvolto e tipo di evento. I log sono essenziali per monitorare la sicurezza dei sistemi: permettono di individuare accessi sospetti, anomalie, minacce informatiche e comportamenti. Garantiscono la tracciabilità necessaria per ricostruire eventi passati: chi ha acceduto ai dati, quando, e cosa è stato fatto. Questi elementi sono vitali anche a fini probatori e di audit.
In ambito GDPR, i log sono strumenti fondamentali di accountability, cioè capacità di dimostrare l'adozione di misure per proteggere i dati personali.

sere copiati e utilizzati senza possibilità di tutela effettiva. Ad esempio, dati sanitari, finanziari e personali diventerebbero accessibili, compromettendo privacy e diritti fondamentali.
I rischi operativi, invece, si manifestano soprattutto in caso di interruzioni o fallimenti del fornitore. Un downtime prolungato di un servizio Cloud di collaboration può bloccare attività aziendali critiche, impedendo ai dipendenti di accedere a documenti e sistemi essenziali. Ancora più problematico è il fenomeno del vendor lock-in: un'azienda che sviluppa soluzioni integrate con un Cloud specifico può trovarsi ostacolata nel migrare i propri dati altrove, con costi elevati e perdita di flessibilità strategica.

In sintesi, i principali rischi connessi alla perdita di controllo dei dati possono essere così riassunti:

- furto o esposizione di dati sensibili a causa di vulnerabilità o accessi non autorizzati;
- violazioni normative legate a conflitti di giurisdizione e mancata conformità (es. GDPR);
- interruzioni operative dovute a guasti, downtime o indisponibilità del provider;
- uso improprio dei dati da parte del provider, in assenza di adeguati vincoli contrattuali.

Rischio di dipendenze tecnologiche

A queste criticità di natura tecnica, legale e organizzativa si aggiunge un ulteriore livello di complessità, legato alla dimensione geopolitica e strategica. La dipendenza tecnologica da piattaforme estere può esporre a ingerenze giuridiche e politiche. Nell'attuale contesto economico mondiale potrebbe succedere che uno Stato subisca le decisioni di un soggetto privato anche in ambiti altamente strategici.

***Esempio**: a marzo 2025 Elon Musk, sul suo social network X, ha dichiarato "Il mio sistema Starlink è la spina dorsale dell'esercito ucraino. Tutta la loro prima linea crollerebbe se lo spegnessi".*

Per chi governa un'azienda è evidente che la diffusione massiva di Intelligenza Artificiale, Internet of Things e Edge computing sta generando volumi di dati senza precedenti, che richiedono tempi di risposta ridottissimi, continuità operativa e una gestione trasparente. Se queste infrastrutture sono controllate da soggetti extra-europei, aumenta il rischio di lock-in: dipendere da un fornitore significa rinunciare alla possibilità di negoziare condizioni, innovazioni e persino il livello di sicurezza. A questo si aggiunge il fattore geopolitico: la pandemia, la guerra in Ucraina e le tensioni commerciali tra Stati Uniti e Cina hanno mostrato quanto le catene del valore globali possano essere fragili.

Se un'intera economia dipende da infrastrutture digitali governate altrove, il rischio di interruzioni diventa non più solo operativo, ma strategico.

La domanda a cui bisogna rispondere per "garantire la solidità dell'infrastruttura strategica Cloud" non è più solo come utilizzare i dati, ma quali tecnologie usare, dove conservarli e, soprattutto, chi può accedervi e con quali regole!

> *È qui che entra in gioco il Cloud Sovrano: un modello che combina la potenza e la flessibilità del Cloud con la garanzia che i dati restino sotto la giurisdizione di chi li produce.*

Capitolo 3

Cosa rende “Sovrano” il Cloud.

Mettiamo in luce che il Cloud Sovrano non coincide con la semplice localizzazione dei dati, ma con la loro piena governance giuridica, tecnologica e operativa. Il Cloud Sovrano si distingue dal Cloud tradizionale perché garantisce che dati, metadati e chiavi crittografiche restino sotto giurisdizione nazionale, proteggendoli da leggi extraterritoriali e accessi non autorizzati. I suoi tre pilastri sono: controllo dei dati, giurisdizione esclusiva e gestione sovrana delle chiavi di cifratura. In definitiva, non è solo un’infrastruttura IT, ma un vero asset strategico che fonda la fiducia di cittadini, imprese e istituzioni.

Intanto cominciamo col dire che non esiste ancora una definizione del concetto di Cloud Sovrano, benché nel Parlamento Europeo si stiano muovendo i primi passi in questa direzione.
Su richiesta della Commissione Europea anche nell’ambito della European Alliance for Industrial Data, Edge and Cloud[10] è stata avviata un’attività sulla definizione del concetto di sovranità applicabile alle infrastrutture Cloud ed Edge[11] in Europa volta a individuare i criteri alla base della sovranità.
L’aggettivo sovrano si presta alla domanda: “rispetto a cosa? E rispetto a chi?”. La sovranità può essere la risposta ad una normativa o una risposta ad un contesto geopolitico, La sola normativa è una base, una condizione necessaria ma non sufficiente. Il concetto di sovranità deve inoltre essere valutato su più dimensioni che includono la disponibilità tecnologica, il trattamento dei dati, l’operatività delle soluzioni, la giurisdizione applicabile.

Gli obiettivi della sovranità

Il Cloud Sovrano rappresenta il “custode digitale” dei dati la cui compromissione può mettere in crisi una organizzazione fino a renderla incapace di svolgere la propria missione. La sua funzione non si limita a fornire capacità di calcolo e archiviazione, ma è quella di garantire che tali dati rimangano sempre sotto il controllo giuridico, operativo e tecnologico del soggetto sovrano.

[10] https://digital-strategy.ec.europa.eu/en/policies/Cloud-alliance
[11] Un’infrastruttura Edge è l’insieme di risorse hardware e software (server, storage, rete, piattaforme applicative) collocate vicino alla fonte dei dati, per elaborare informazioni in tempo reale senza doverle inviare sempre al Cloud. È composta da:
• Dispositivi e sensori (IoT, macchinari, veicoli, smartphone) che generano i dati.
• Nodi Edge (gateway, server locali, micro-data center) che elaborano, filtrano e archiviano i dati vicino alla loro origine.
• Rete di connettività (LAN, Wi-Fi, 5G, reti dedicate) che collega dispositivi, Edge e Cloud.
• Cloud e data center centrali per analisi più complesse, archiviazione e addestramento di modelli.
• Piattaforme di orchestrazione che gestiscono applicazioni, sicurezza e monitoraggio dei nodi distribuiti.
L’infrastruttura Edge porta potenza di calcolo e servizi digitali più vicino agli utenti e ai dispositivi, riducendo latenza, costi di banda e rischi di sicurezza, e complementando il Cloud con una rete distribuita di nodi locali.

In sintesi, la sovranità si caratterizza quando risolve i seguenti temi chiave:

- **Localizzazione e controllo dei dati**

I dati devono risiedere in data center situati all’interno dei confini dell’area caratterizzata dalla medesima giurisdizione. La localizzazione non è solo geografica, ma anche logica: significa che la gestione delle copie, dei backup e della replicazione deve avvenire in un perimetro controllabile.

- **Giurisdizione esclusiva**

Nessuna autorità straniera deve poter obbligare i provider a fornire i dati, senza il consenso del proprietario ed il coinvolgimento delle autorità della nazione.
Questo protegge da normative extraterritoriali come il Cloud Act USA o la National Intelligence Law cinese, che impongono l’accesso ai dati anche se conservati altrove.

- **Controllo delle chiavi crittografiche e in ultimo controllo della sicurezza**

Le chiavi di cifratura e gli applicativi del Cloud non possono essere gestite da un provider globale estero, né direttamente né indirettamente. Devono rimanere sotto la giurisdizione del soggetto sovrano.

Il controllo delle chiavi è infatti il vero “grimaldello”: chi le possiede può accedere ai dati, anche se cifrati. In un Cloud davvero “sovrano”, le chiavi di crittografia devono essere create, gestite e distribuite da soggetti certificati che abbiano piena autonomia, anche rispetto ai contratti con i propri clienti, e che non siano sottoposti a giurisdizioni straniere. Solo così si evita il paradosso che i sistemi crittografici, nati per impedire l’accesso ai dati a chi non ne ha diritto, finiscano invece per renderli leggibili a terzi legalmente. Questo potrebbe concretamente avvenire quando, per legge, le chiavi devono essere consegnate a un’autorità straniera che ha potere legale sulle aziende sotto la sua giurisdizione, anche se queste operano in altri Paesi.

Come il Cloud Sovrano si differenzia da un Cloud tradizionale

Nel Cloud pubblico tradizionale, le informazioni possono essere replicate in più Paesi per motivi di performance o ridondanza. Inoltre, la legge applicabile è spesso quella della sede legale del provider, non quella in cui si trova il cliente. Questo crea incertezza normativa e rischi di esposizione a giurisdizioni estere.

Il Cloud Sovrano ribalta questa logica:

- la sede legale e la giurisdizione coincidono con il territorio in cui i dati risiedono;
- la replicazione è limitata a confini controllati, o che comunque rispettino la sovranità d’origine;
- le chiavi di cifratura sono gestite solo da entità sovrane, siano esse pubbliche o private;
- la rete di comunicazione al Cloud è a sua volta “sovrana” (vedi sopra).

Un fraintendimento diffuso è pensare che la sovranità significhi “chiusura tecnologica”.

> *In realtà, i modelli più avanzati integrano tecnologie globali ma le incardinano in una governance nazionale, garantendo interoperabilità senza perdere il controllo.*

La dimensione della fiducia

Alla base del Cloud Sovrano c’è un concetto trasversale: la fiducia.

- I cittadini devono poter avere fiducia che i propri dati sanitari o fiscali non saranno accessibili a potenze straniere.
- Le imprese devono avere fiducia che i loro segreti industriali non possano essere sottratti o usati per vantaggi competitivi altrui.
- Le istituzioni devono poter pianificare strategie di difesa e sicurezza senza il rischio che tali informazioni diventino vulnerabili.
- Gli utenti di qualsiasi tipo devono essere certi che nessuno interromperà la funzionalità degli applicativi forniti in modalità SaaS ed accederà ai dati degli stessi senza il permesso delle leggi sovrane del paese in cui risiede.

> *In questo senso, il Cloud Sovrano non è solo un’infrastruttura tecnologica, ma un asset strategico nazionale: il luogo digitale in cui si custodisce il capitale informativo di un Paese.*

In conclusione, un’infrastruttura di Cloud Sovrano riduce l’esposizione a rischi informatici, perché mantiene i dati rilevanti in un perimetro giuridico controllato, con standard di sicurezza uniformi e procedure di risposta alle crisi coordinate. In questa ottica un Cloud Sovrano è, di fatto, un bene infrastrutturale critico, al pari di reti elettriche, dei sistemi di trasporto e approvvigionamento energetico, perché abilita la sicurezza nazionale delle imprese e l’indipendenza strategica di un Paese o di un’intera area geopolitica come l’Unione Europea. Come il petrolio ha alimentato la rivoluzione industriale, così i dati alimentano la rivoluzione digitale. Con una differenza sostanziale: questa volta abbiamo la possibilità - e la responsabilità - di decidere fin da subito come proteggere e utilizzare questa risorsa.
Per questo motivo la sovranità digitale non è un concetto astratto, ma una condizione necessaria per garantire innovazione, sicurezza e libertà economica. Non si tratta di isolarsi dal resto del mondo, ma di stabilire regole chiare: apertura tecnologica, sì; vulnerabilità strategica, no.

Capitolo 4

Il contesto normativo internazionale e europeo.

L'adozione del Cloud Sovrano è una priorità globale: gli USA dominano il mercato ma con il vincolo del Cloud Act, l'Asia rafforza il controllo statale e il Medio Oriente investe per diventare hub regionale. L'Europa, pur dotata di norme come GDPR e Data Act, resta indietro per assenza di hyperscaler propri e frammentazione regolatoria, rischiando dipendenza da infrastrutture extra-UE. Per garantire sicurezza, competitività e autonomia, l'UE deve agire subito con investimenti mirati, partnership pubblico-private e riconoscimento del Cloud Sovrano come infrastruttura critica.

Il Cloud Sovrano è ormai una priorità in diverse aree del mondo. Ogni Paese lo interpreta in base alla propria posizione geopolitica, al livello di maturità digitale e alle proprie esigenze di sicurezza. Il contesto normativo pone le basi per verifiche oggettive ma va contestualizzato nello scenario geopolitico di riferimento. Infatti, spesso, il contesto normativo si pone come ago della bilancia tra necessità di regolare e necessità di garantire un libero mercato. Vediamo la situazione internazionale.

Nord America: leadership tecnologica e controllo giuridico

Gli USA dominano il mercato globale del Cloud grazie a hyperscaler come AWS, Microsoft, Google e Oracle, unitamente ai player del software as a service (es. Salesforce, ServiceNow etc)
La legge Cloud Act obbliga i provider statunitensi a fornire dati al governo USA su richiesta, ovunque essi siano conservati e soprattutto senza nessun tipo di comunicazione verso le autorità o i soggetti dei paesi terzi. In altri termini, il Cloud Act agisce sulla titolarità effettiva del dato creando un conflitto non risolto con il GDPR.
Questa impostazione crea possibili tensioni con le leggi di protezione dei dati di altri Paesi (es. GDPR in Europa) perché può obbligare un provider a consegnare informazioni che localmente sarebbero protette. In tal senso, le aziende che usano provider USA devono considerare il rischio che i loro dati possano essere richiesti dalle autorità statunitensi, indipendentemente dalla localizzazione fisica dei server.
Ciò sta inducendo l'Europa ad accelerare sulla creazione di alternative sovrane.

Asia: modelli chiusi e controllo statale

La Cina ha puntato su una fortissima regolamentazione a protezione dei trasferimenti transfrontalieri dei dati e infrastrutture totalmente controllate dal governo. Si tratta di un modello cosiddetto Modello "Full Sovereign" perché l' infrastruttura è interamente progettata, costruita e gestita a livello nazionale.
In India, le politiche di localizzazione dati sono state adottate per rafforzare l'industria ICT locale.

Medio Oriente: hub regionali e investimenti massicci

Emirati e Arabia Saudita stanno investendo miliardi per diventare hub tecnologici regionali, attirando hyperscaler con vincoli di localizzazione cui vengono fatte però corrispondere garanzie per il mantenimento della sovranità digitale "nativa" dell'investitore. Si tratta di un modello cosiddetto "Joint Venture" perché prevede la collaborazione tra provider globale e operatore locale certificato.

Europa: cooperazione e frammentazione

L'Europa ancora oggi soffre di un doppio gap:

- **Tecnologico**

Non esistono hyperscaler nativi europei in grado di competere con i giganti globali.

- **Regolatorio**

Regole frammentate e lente rispetto alla velocità della competizione globale.

Negli ultimi 10 anni sono stati introdotti strumenti come GDPR, Data Governance Act, Data Act e NIS2, ma queste norme non offrono una cornice definita sul tema del Cloud Sovrano. Per questo motivo, la Commissione intende introdurre il Cloud and AI Development Act, parte del più ampio AI Continent Action Plan[12]. Questo disegno di legge mira a:

- triplicare la capacità di elaborazione dati dell'UE entro il 2030;
- favorire Cloud sovrani strategici, soprattutto con la pubblica amministrazione come client ancoraggio;
- introdurre preferenze in appalti pubblici per fornitori europei;
- accelerare la costruzione di infrastrutture Cloud ed Edge, sostenute da incentivi e capitali pubblici.

Il modello che delinea la Commissione europea favorisce una soluzione "federata" perché prevede una rete di infrastrutture interoperabili che rispettino standard comuni e siano soggette ad una giurisdizione unica ed insieme forniscano una massa critica sufficiente a competere nel mercato.
Lo svantaggio di questo modello è legato alla complessità di governance e coordinamento.

> *"La sfida dei prossimi anni sarà trovare l'equilibrio tra condivisione globale e controllo nazionale, tra interoperabilità e indipendenza, tra crescita tecnologica e tutela strategica, tra protezionismo e contaminazione tecnologica."*

[12] La consultazione pubblica sul Cloud and AI Development Act si è conclusa a giugno 2025.

Riguardo all'evoluzione normativa europea è bene ricordare alcuni rilevanti interventi finalizzati a mettere in evidenze la "discontinuità" che l'Europa deve affrontare per risolvere le debolezze attuali e quelle ancor più importanti che si prospettano in futuro.
Nel Rapporto Draghi sulla competitività dell'Unione Europea si evidenzia che "non si può abbandonare il controllo in ambiti cruciali come la sicurezza e la crittografia", nonostante "lo svantaggio competitivo dell'UE nel Cloud computing".
"È importante che le aziende europee mantengano una presenza in settori dove è necessaria la sovranità tecnologica, come la sicurezza e la crittografia, attraverso soluzioni di "Cloud Sovrano".
Anche il Presidente della Repubblica Italiana, Sergio Mattarella, ha richiamato l'attenzione sullo squilibrio crescente tra potere privato e potere pubblico invocando la necessità di «regole che riconducano al bene comune lo straripante peso delle corporazioni globali – quasi nuove Compagnie delle Indie – che si arrogano l'assunzione di poteri che si pretende che Stati e Organizzazioni internazionali non abbiano a esercitare»[13]
Intanto, poiché l'approvazione del Cloud and AI Development Act sarà fortemente soggetta a negoziazioni e pressioni esterne, Francia e Germania proprio di recente hanno accelerato sul tema della sovranità rappresentando una posizione comune e ponendo le basi per mobilitare investimenti e progetti comuni subito, senza attendere i tempi legislativi UE.

Con l'accordo bilaterale del 1° settembre 2025, Francia e Germania cercano di rafforzare la linea di un Cloud Sovrano nel dibattito[14] sottolineando la necessità di:

- costruire un'infrastruttura digitale sicura e aperta, fondata su valori europei e capace di ridurre dipendenze esterne;
- promuovere una strategia Multi Cloud europea, con un "perno locale" europeo;
- organizzare un summit per mobilitare risorse e coordinare investimenti digitali entro novembre 2025;
- favorire un ecosistema digitale pubblico-europeo, integrando soluzioni nazionali come Suite numérique e OpenDesk[15].

[13] L'intervento (videomessaggio) del Presidente Sergio Mattarella è stato diffuso nella giornata di sabato 6 settembre 2025 ed è stato realizzato in occasione del Forum Ambrosetti di Cernobbio.
[14] L'agenda economica franco-tedesca che contiene la posizione comune su Cloud Sovrano e digitale è stata pubblicata e firmata il 1° settembre 2025 a Parigi, nell'ambito dell'incontro bilaterale tra Emmanuel Macron e Olaf Scholz.
[15] Suite numérique (Francia) è un insieme di strumenti digitali open source e sovrani sviluppati in Francia per le pubbliche amministrazioni. Comprende applicazioni per posta elettronica, collaborazione, videoconferenza, gestione documentale e produttività d'ufficio. L'obiettivo è ridurre la dipendenza da suite proprietarie straniere (come Microsoft 365 o Google Workspace) e garantire sovranità dei dati e conformità al GDPR. È promosso dall'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) e dal Ministero della Funzione Pubblica.
OpenDesk (Germania) è l'equivalente tedesco: una piattaforma che integra software open source certificato per l'uso nelle amministrazioni pubbliche federali e locali. Include strumenti per email, office automation, videoconferenze, gestione collaborativa (spesso basati su soluzioni come NextCloud, LibreOffice, Matrix). Nasce per garantire interoperabilità, sicurezza e per costruire un ecosistema digitale federato indipendente da vendor extraeuropei.

La regolamentazione italiana

Con la Strategia Cloud Italia (2021) e le successive determine ACN del 2022, l'Italia ha introdotto una regolamentazione per guidare la migrazione delle Pubbliche Amministrazioni verso un modello di Cloud sicuro e sovrano.

Gli obiettivi principali erano:

- garantire la protezione e il controllo giurisdizionale dei dati più sensibili;
- definire una classificazione dei dati con vincoli proporzionati al livello di rischio;
- creare un'infrastruttura nazionale di riferimento, il Polo Strategico Nazionale (PSN).

Il PSN è stato concepito come una piattaforma nazionale, con caratteristiche distintive:

- giurisdizione italiana ed europea, per evitare esposizione a normative extra-UE (es. Cloud Act USA);
- affidabilità e resilienza, grazie a una rete di data center distribuiti sul territorio;
- standard elevati di sicurezza, definiti dall'Agenzia per la Cybersicurezza Nazionale (ACN);
- flessibilità tecnologica, con soluzioni Cloud private, ibride, IaaS e PaaS, pensate per interoperabilità e scalabilità.

Il PSN poggia su competenze tecnologiche nazionali:

- esperienza consolidata in gestione di data center, cybersecurity, reti e architetture Cloud;
- coinvolgimento di attori pubblici e privati con forte know-how ICT;
- integrazione con le linee guida AgID;
- ACN come autorità centrale che definisce regole, standard e processi di qualificazione.

La normativa ha distinto tre livelli di gestione dei dati, ciascuno con obblighi specifici:

- **Dati ordinari** (non critici per la sicurezza nazionale)

Ospitabili su Cloud pubblici qualificati, anche di fornitori internazionali conformi alle regole ACN.

- **Dati critici** (riguardano servizi essenziali, es. sanità, finanza, trasporti)

Possono essere gestiti anche fuori dal PSN, purché su Cloud qualificati con requisiti elevati di sicurezza e resilienza.

- **Dati strategici** (coinvolgono funzioni vitali per la sicurezza nazionale)

Devono risiedere obbligatoriamente nel PSN o in infrastrutture equivalenti sotto piena giurisdizione italiana/UE.

I limiti principali della attuale regolamentazione italiana sul Cloud Sovrano possono essere così sintetizzati:

- **Perimetro ristretto**

La normativa si concentra sulla Pubblica Amministrazione sui cui è focalizzato il Polo Strategico Nazionale. Questo è un limite perché lascia intendere che il tema della governance dei dati sia rilevante solo per la PA. Settori industriali strategici come energia, telecomunicazioni, sanità, finanza, trasporti devono invece essere parte del perimetro sovrano. Anche le piccole e medie imprese (PMI) che operano in filiere critiche devono poter accedere a un Cloud che risponde alla giurisdizione sovrana, con soluzioni scalabili e costi sostenibili.

- **Possibilità di ricorso all'uso degli hyperscaler stranieri per i dati "ordinari" e "critici"**

La regolamentazione consente alle PA di utilizzare applicativi e servizi di grandi provider globali (AWS, Microsoft, Google), che restano soggetti a normative extra-UE (es. Cloud Act USA). Ne consegue che gli stessi possono essere obbligati alla consegna o decriptazione dei dati sensibili, anche se fisicamente conservati in Italia perché non esiste un divieto esplicito di trasferimento transfrontaliero per i dati critici, secondo la definizione ACN. Ciò indebolisce il principio di "sovranità dei dati", perché la loro protezione dipende da accordi contrattuali e non da una barriera giuridica assoluta. C'è un controllo giurisdizionale incerto: se un'applicazione in Cloud Sovrano integra componenti software estere, la giurisdizione locale potrebbe essere aggirata, esponendo i dati a richieste legali o accessi forzati da parte di governi stranieri.

- **Asimmetria normativa**

Mentre la regolamentazione italiana impone compliance alla PA, non impone ai fornitori globali di adattare pienamente i propri modelli giuridici e tecnici alla giurisdizione nazionale. Sussiste, quindi, una sostanziale asimmetria normativa.

> *"In sintesi, secondo la regolamentazione attuale sottostante al PSN il rischio è che la sovranità formale (il dato è "in Italia") non corrisponda a una sovranità sostanziale, perché, secondo l'attuale normativa, il controllo ultimo dei dati critici potrebbe restare nelle mani di soggetti esteri."*

A queste "fragilità" il Polo Strategico Nazionale ha reagito adottando pratiche di governance dei dati basate sui contratti e sulla gestione del personale. Infatti, gli accordi con hyperscaler prevedono la gestione esclusiva dei dati in capo al Polo stesso e al suo personale.

Capitolo 5

Casi e buone pratiche.

Illustriamo le esperienze internazionali (Francia, Germania, Australia, Brasile) individuando fattori di successo come governance chiara, approccio modulare e standard aperti. L'esperienza internazionale dimostra che il Cloud Sovrano è una realtà già in corso di attuazione. Analizzare modelli e risultati di Paesi che hanno intrapreso questo percorso permette di identificare strategie vincenti ed errori da evitare.

L'esperienza internazionale mostra che il Cloud Sovrano non è più una teoria, ma una realtà già operativa in diversi Paesi. Ogni modello riflette priorità specifiche - sicurezza, sviluppo industriale, attrazione investimenti - ma tutti hanno un punto in comune: la volontà di garantire controllo strategico sui dati più sensibili.

Francia – Il modello "Cloud de Confiance"

La Francia è stata tra i primi Paesi europei a introdurre un modello ibrido di sovranità digitale.

- Contesto: nel 2021 il governo francese ha definito il "Cloud de Confiance" come soluzione per proteggere i dati sensibili di PA e imprese strategiche[16].
- Approccio: utilizzo di tecnologie globali (Microsoft Azure, Google Cloud), ma operate e gestite da aziende francesi certificate (OVH, Orange, Capgemini).
- Risultati concreti: nascita della joint venture Bleu (Orange + Capgemini + Microsoft), che già fornisce servizi Cloud certificati a ministeri, ospedali e banche; creazione di oltre 37.000 posti di lavoro qualificati nella filiera ICT francese[17]; standard di sicurezza definiti dall'agenzia nazionale ANSSI come riferimento per tutti i provider.

***Lezione chiave**: è possibile conciliare innovazione globale e governance locale, a patto che i ruoli siano chiaramente definiti.*

[16] La circolare del 5 luglio 2021 del governo francese formalizza la dottrina "Cloud au centre", che impone alle amministrazioni di affidarsi a Cloud "di fiducia" (Cloud de confiance) certificati ANSSI SecNumCloud per i dati sensibili https://www.economie.gouv.fr/securite-performance-souverainete-strategie-Cloud

[17] https://www.anrt.asso.fr/sites/default/files/2024-03/ANRT_Digital_sovereignty_regaining_control_in_France_and_Europe_01.24.pdf

Germania – GAIA-X e il modello federato

La Germania ha puntato su un'infrastruttura federata e aperta.

- Contesto: GAIA-X nasce nel 2019 come iniziativa congiunta franco-tedesca, oggi supportata da oltre 300 aziende europee[18].
- Approccio: ogni Paese mantiene i propri data center e la propria governance, ma adotta standard tecnici comuni (API, protocolli di sicurezza, sistemi di certificazione).
- Progetti pilota: condivisione sicura di dati sanitari tra ospedali in UE, con riduzione del 15% di spesa ospedaliera[19]; progetti Industry 4.0 che connettono fabbriche intelligenti in diversi Paesi, migliorando l'efficienza produttiva fino al 30%.[20]
- Risultati concreti: definizione di un framework di compliance che è diventato riferimento anche per operatori non europei.

***Lezione chiave**: la standardizzazione garantisce interoperabilità e scalabilità.*

Australia – Data Sovereignty per infrastrutture critiche

L'Australia ha scelto un approccio selettivo e settoriale.

- Normativa: Security of Critical Infrastructure Act, che impone la conservazione dei dati relativi a energia, sanità, telecomunicazioni e difesa all'interno dei confini nazionali.[21]
- Approccio: focus su settori critici, senza imporre la sovranità a tutta l'economia.
- Risultati concreti: maggiore fiducia degli investitori nel settore energetico e sanitario; riduzione significativa degli incidenti di cybersecurity nelle infrastrutture critiche; tempi di risposta agli attacchi ridotti fino al 30% grazie a data center locali.[22]

***Lezione chiave:** partire dai comparti più sensibili è un modo rapido per ottenere benefici concreti e ridurre i costi iniziali.*

[18] https://www.agendadigitale.eu/infrastrutture/gaia-x-il-Cloud-europeo-per-dare-un-futuro-alle-imprese-italiane/
[19] Fonte: "Measuring the economic impact of Cloud computing in Europe" – European Commission
[20] https://web-assets.bcg.com/img-src/Industry_40_Future_of_Productivity_April_2015_tcm9-61694.pdf
[21] https://bosscap.com.au/media-release/the-security-of-critical-infrastructure-act-soci-protects-us-from-unimaginable-chaos/
[22] https://versent.com.au/case-studies/versent-assists-an-australian-state-department-to-securely-govern-land-planning-data-with-aws-Cloud-solutions/

Brasile – Incentivi economici e filiera locale

Il Brasile ha adottato un modello pragmatico e orientato allo sviluppo industriale.

- Normativa chiave: la LGPD (Legge Generale sulla Protezione dei Dati), ispirata al GDPR europeo.
- Approccio: incentivare la costruzione di data center locali tramite sgravi fiscali e agevolazioni burocratiche, attirando sia hyperscaler globali sia startup nazionali.
- Il progetto "Nuvem do Brasil": una infrastruttura di Cloud per la PA con un modello di Cloud ibrido molto simile a quello realizzato in Italia dal PSN.
- Risultati concreti: aumento del numero di data center Tier III e IV sul territorio; creazione di migliaia di posti di lavoro qualificati nel settore ICT; crescita della spesa in R&D da parte dei provider globali, spinti dalle condizioni favorevoli.

***Lezione chiave**: incentivare gli investiti sulle infrastrutture come i data center a livello locale può essere un punto chiave della strategia sul Cloud Sovrano.*

Italia - Il Polo Strategico Nazionale

Come detto nel precedente capitolo la regolamentazione nazionale presenta alcune debolezze rispetto alla sovranità; tuttavia, il modello di servizio del PSN rappresenta anche una best practice perché risponde ad una serie di obiettivi strategici nazionali. Si tratta, infatti di un'iniziativa prevista dal Piano Nazionale di Ripresa e Resilienza (PNRR) che ha l'obiettivo di migrare gran parte dei dati e servizi critici della Pubblica Amministrazione in un'infrastruttura Cloud sicura e certificata.
Il PSN assicura una serie di vantaggi: i grandi operatori privati (es. TIM, Leonardo, Sogei, CDP nel caso del PSN) portano know-how tecnologico, esperienze di mercato e infrastrutture già consolidate come i data center di livello enterprise; ciò ha ulteriormente accelerato lo sviluppo di piattaforme sicure e moderne, evitando che lo Stato dovesse svilupparle interamente da zero. Questo approccio è cruciale in progetti con vincoli di tempo e risorse.
A ciò si aggiunge che il modello regolamentare, indebolito dalla possibilità di trasferimento dei dati critici all'estero, è tuttavia reso più solido in termini di sovranità dalla presenza di accordi con hyperscaler che prevedono l'esclusiva giurisdizione della gestione del dato da parte del personale del PSN. Ciò garantisce in sostanza che i dati restino sotto giurisdizione italiana, le policy di sicurezza siano definite dallo Stato, non ci siano rischi di extraterritorialità (es. Cloud Act USA).

***Lezione chiave**: valorizzare le competenze di player nazionali ha consentito di accelerare il raggiungimento degli obiettivi di sovranità sui dati della Pubblica Amministrazione.*

Capitolo 6

Sfide e criticità.

Analizziamo le difficoltà: alti costi iniziali, dipendenza tecnologica, problemi di interoperabilità, carenza di competenze e normative in evoluzione.

L'adozione del Cloud Sovrano porta benefici rilevanti, ma richiede di affrontare sfide tecniche, economiche e normative. La sostenibilità di lungo periodo dipende dalla capacità di bilanciare sicurezza, apertura tecnologica e competitività.

Costi e investimenti iniziali

Costruire un'infrastruttura sovrana richiede capitali significativi. Data center di ultima generazione, sistemi di cybersecurity avanzati, sistemi sovrani per la gestione delle chiavi di crittografia, personale specializzato e certificazioni di sicurezza sono voci di spesa rilevanti.
Molti governi e imprese devono affrontare il dilemma tra investire subito in autonomia o continuare a usare soluzioni esistenti, con i relativi rischi.

Accesso alle tecnologie più avanzate

Gli hyperscaler globali investono miliardi in ricerca e sviluppo, mantenendo un vantaggio tecnologico notevole. Un'infrastruttura sovrana rischia di rimanere indietro se non integra innovazioni come AI generativa, machine learning distribuito e servizi Cloud-native di ultima generazione.
Una forte spinta europea al recupero del ritardo accumulato, con progetti come Eurostack o altre politiche industriali a sostegno, è necessaria per rendere nel lungo periodo il Cloud europeo competitivo con gli hyperscalers. Nel breve medio-periodo, occorre stabilire partnership strategiche che salvaguardino la sovranità pur garantendo l'accesso a tecnologie di frontiera.

Interoperabilità e standard

Il rischio di frammentazione tecnologica è concreto. Senza standard condivisi, un Cloud Sovrano potrebbe isolarsi dal resto dell'ecosistema digitale, rendendo più difficile l'integrazione con partner internazionali e limitando la scalabilità dei servizi.
L' Europa è ora impegnata per mitigare questo rischio promuovendo specifiche tecniche comuni. A tale scopo è necessario favorire in Europa un approccio cooperativo tra le aziende (come avviene nel programma europeo IPCEI CIS) che getti le basi per un'interoperabilità delle soluzioni Cloud in un contesto di sovranità.

Competenze e talenti

La gestione di un'infrastruttura sovrana richiede competenze avanzate in cybersecurity, Cloud architecture, crittografia e governance dei dati.
La carenza di profili specializzati è una criticità globale: senza una strategia di formazione e attrazione dei talenti, il rischio è quello di avere infrastrutture sicure sulla carta, ma vulnerabili nella gestione quotidiana.
Ma attenzione, le aziende sovrane devono essere messe in grado di retribuire adeguatamente le professionalità specialistiche. Oggi così non è, con il rischio che l'investimento in formazione, slegato da una politica industriale strategica, finisca per riempire di foraggio i granai dei nostri competitor, perché i giovani italiani vanno a lavorare all'estero e molto spesso fuori dall'UE.

Evoluzione normativa

Le leggi sulla protezione dei dati, la cybersicurezza e l'Intelligenza Artificiale sono in continua evoluzione. Il tema della sovranità del Cloud in particolare sta guadagnando un'attenzione crescente in Europa, nell'ambito dello schema di certificazione della cybersicurezza per i servizi Cloud (EUCS) e della imminente iniziativa legislativa Cloud and AI Development Act. Un'infrastruttura sovrana deve essere progettata per adattarsi rapidamente a nuovi requisiti normativi, evitando lock-in regolatori o costosi aggiornamenti.

> *Il Cloud Sovrano è una scelta strategica che comporta sfide non trascurabili. La chiave del successo è un approccio graduale e modulare, capace di crescere nel tempo senza compromettere sicurezza e interoperabilità.*

Capitolo 7

I benefici del Cloud Sovrano, l'impatto sull'economia.

Il Cloud Sovrano non è soltanto un presidio di sicurezza: è una leva strategica per la resilienza, la competitività e la fiducia digitale. La sua adozione genera vantaggi tangibili: tutela della sicurezza nazionale, continuità operativa, stimolo agli investimenti, attrazione di talenti e capitali, sostegno all'innovazione, creazione di occupazione qualificata, rafforzamento delle filiere tecnologiche locali, conformità normativa e sostenibilità ambientale.

Il Cloud Sovrano rappresenta un investimento strategico che moltiplica valore infrastrutturale, economico, sociale e ambientale. Vediamo perché.

Sicurezza nazionale e protezione dei dati strategici

In un mondo iperconnesso, i dati sono una risorsa critica per la sicurezza nazionale. Piani di difesa, progetti di ricerca, infrastrutture energetiche e sistemi sanitari devono essere protetti da accessi non autorizzati e da normative extraterritoriali.

Il Cloud Sovrano garantisce che la gestione delle chiavi crittografiche resti sotto giurisdizione nazionale o comunitaria, azzerando il rischio di interferenze estere.

Resilienza operativa in scenari di crisi

Crisi geopolitiche, tensioni commerciali o attacchi informatici possono compromettere l'accesso a dati critici se custoditi all'estero.

Il Cloud Sovrano assicura continuità grazie a:

- servizi applicativi in modalità SaaS con garanzia di disponibilità;
- data center ridondati sul territorio nazionale o europeo;
- procedure di disaster recovery sotto pieno controllo locale;
- capacità di isolamento rapido in caso di attacco, senza interruzioni ai servizi essenziali.

Rappresenta quindi un "piano B" permanente, a tutela della stabilità del sistema Paese.

Stimolo agli investimenti e creazione di filiere locali

La progettazione di un Cloud Sovrano comporta la costruzione di nuovi data center, l'aggiornamento delle reti in fibra e 5G e lo sviluppo di piattaforme software sicure. Questi investimenti mobilitano risorse significative e generano effetti moltiplicatori sull'economia.

***Evidenza**: secondo IDC, ogni dollaro investito in infrastrutture Cloud può generare fino a 6,7 dollari nell'economia locale.*

***Esempio**: in Francia, il programma Cloud de Confiance ha attivato oltre 600 milioni di euro in nuovi data center, coinvolgendo decine di fornitori locali.*

Il Cloud Sovrano stimola inoltre la nascita di un ecosistema di fornitori nazionali nei settori hardware, software e servizi, riducendo la dipendenza dall'estero e rafforzando la resilienza delle supply chain.

Occupazione qualificata e sviluppo delle competenze

Un'infrastruttura sovrana richiede competenze specialistiche: Cloud architect, ingegneri di sicurezza informatica, esperti di crittografia, data governance officer e project manager.

***Evidenza**: KPMG stima che il settore Cloud potrebbe generare in Europa oltre 500.000 nuovi posti di lavoro qualificati entro il 2027, molti dei quali legati a progetti di sovranità digitale.*

***Esempio**: il programma GAIA-X ha avviato collaborazioni con università e centri di ricerca per formare professionisti dedicati alla gestione di Cloud federati.*

Accelerazione dell'innovazione

Il Cloud Sovrano fornisce un ambiente sicuro per sperimentare tecnologie emergenti, riducendo i rischi di fuga o uso improprio dei dati:

- industria 4.0: interconnessione sicura delle fabbriche e analisi predittiva della produzione;
- mobilità smart: gestione dei dati di veicoli connessi e infrastrutture di trasporto;
- sanità digitale: analisi congiunta dei dati medici su scala europea nel rispetto delle norme nazionali.

Conformità normativa e riduzione dei rischi legali

In un perimetro giuridico chiaro, senza conflitti di legge, i processi di gestione e archiviazione risultano più trasparenti ed efficienti. Ne derivano minori rischi di sanzioni, procedure semplificate e maggiore fiducia da parte di clienti e partner.

Fiducia e reputazione

La protezione dei dati è anche un asset reputazionale. Un'infrastruttura sovrana comunica affidabilità e responsabilità, rafforzando il rapporto con cittadini, imprese e stakeholder. In un'epoca di fragilità della fiducia digitale, questo è un vantaggio competitivo decisivo.

Rafforzamento della competitività internazionale

Un Paese con infrastrutture digitali sicure e sotto controllo locale è più attrattivo per investitori, centri di ricerca e partner commerciali. C'è un fattore reputazionale legato alla garanzia di compliance normativa e protezione dei dati e un vantaggio negoziale che porta a una maggiore capacità di stipulare accordi tecnologici da una posizione di forza.

***Evidenza**: i Paesi con strategie strutturate di sovranità Cloud tendono a posizionarsi più in alto nei ranking di resilienza digitale, attirando più investimenti esteri.*

Sostenibilità ambientale

I nuovi progetti di Cloud Sovrano sono spesso progettati con criteri di efficienza energetica e uso di fonti rinnovabili. L'efficienza energetica viene monitorata e governata attraverso indicatori come il PUE (Power Usage Effectiveness), che misura quanto è efficiente l'uso dell'energia in un data center e attraverso il WUE (Water Usage Effectiveness) che misura l'efficienza nell'uso dell'acqua, soprattutto per raffreddare le infrastrutture. L'energia elettrica viene approvvigionata attraverso sistemi di autoproduzione e contratti con fornitori di energia con coinvestimento (PPE con coinvestimento). Questi due aspetti evitano che la crescita esponenziale dei dati gestiti comporti anche un incremento esponenziale dei costi dell'energia.
Inoltre, vengono spesso progettati sistemi di raffreddamento ad aria esterna (free cooling) e recupero del calore generato dai server per uso industriale o residenziale.
Il vantaggio nell'adozione di criteri di sostenibilità ambientale può consistere anche nell'accesso a finanziamenti green.

***Evidenza**: il progetto GAIA-X prevede metriche di sostenibilità per monitorare e ridurre l'impatto ambientale dei data center membri.*

Se ben implementato, il Cloud Sovrano posiziona un Paese come hub digitale sicuro, innovativo e sostenibile, rafforzando la sovranità digitale europea.

In conclusione, il Cloud Sovrano non è un costo da sostenere, ma un investimento strategico che moltiplica valore: infrastrutturale, tecnologico, sociale e ambientale. È una leva di competitività nazionale che, se ben implementata e supportata, posiziona un Paese come hub digitale sicuro e innovativo nel panorama globale.

Capitolo 8

Visione futura e raccomandazioni.

Mettiamo in evidenza come il Cloud Sovrano sia un'infrastruttura strategica, destinata a evolvere entro il 2035 integrando AI, quantum computing, Edge e blockchain. L'Italia parte dal PSN, ma deve estendere il modello oltre la PA, coinvolgendo imprese e settori strategici e superando i limiti sulla governance dell'attuale regolamentazione. Centrale è l'interconnessione: alleanze digitali tra Paesi democratici, modelli federati europei e corridoi sicuri di scambio dati faranno del Cloud una "rete delle reti" sotto controllo locale. Governance adattiva, compliance by design e capitale umano specializzato sono leve essenziali, insieme a data center sostenibili.

Il Cloud Sovrano non è un progetto a termine, ma un'infrastruttura strategica destinata a segnare il prossimo decennio. Al pari delle reti energetiche e dei sistemi di trasporto, diventerà un bene pubblico critico, indispensabile per garantire sicurezza, crescita e competitività.
L'Italia, con il Polo Strategico Nazionale (PSN), parte da una posizione di vantaggio. Ma questa è solo la prima tappa: occorre allargare la visione, superando i confini della sola Pubblica Amministrazione e proteggere l'intero ecosistema produttivo e sociale.

Evoluzione tecnologica: il Cloud del 2035

Il Cloud non resterà immutato: entro il 2035 sarà la piattaforma che integra le tecnologie emergenti.

- **Intelligenza Artificiale Generativa**

I sistemi di AI non saranno solo utilizzatori di dati, ma parte integrante della governance Cloud: automazione della sicurezza, analisi predittiva degli attacchi, ottimizzazione dinamica delle risorse.

- **Quantum computing ed effetti sulla crittografia**

I data center dovranno essere progettati per resistere a computer quantistici capaci di violare le attuali tecniche di cifratura. Come evidenziato nel Capitolo 2, i computer quantistici mettono a rischio gli algoritmi di cifratura oggi utilizzati (RSA, ECC, Diffie-Hellman). Per questo i Cloud sovrani del futuro dovranno integrare crittografia post-quantistica e tecniche che permettono di resistere a nuovi meccanismi di calcolo. Tecnologie come la Quantum Key Distribution (QKD) o la PQC (Post-Quantum Cryptography) saranno fondamentali per garantire la resilienza anche contro minacce che emergeranno nei prossimi decenni. La preparazione oggi è indispensabile per evitare che dati archiviati vengano violati domani, quando la tecnologia quantistica sarà matura.

- **Edge sovrano**

L'elaborazione sempre più vicina alla fonte (ospedali, fabbriche, trasporti) richiederà micro-data center locali certificati, che dialogano con il Cloud centrale ma sotto giurisdizione nazionale.

- **Blockchain e ledger distribuiti**

Per assicurare tracciabilità e audit trasparenti dei processi, dalla logistica alla sanità.

***Raccomandazione**: progettare infrastrutture future-proof, modulari e aggiornabili, capaci di integrare tecnologie ancora in fase sperimentale.*

Sovranità e geopolitica digitale

La sovranità non equivale a isolamento. Nei prossimi anni sarà decisivo costruire alleanze digitali tra Paesi che condividono valori democratici e standard di sicurezza.

In Europa: programmi comunitari (come IPCEI CIS e la European Alliance for Industrial Data, Edge and Cloud) per la creazione di modelli federati, che permettono interoperabilità mantenendo il controllo locale, costruendo così la "rete delle reti" sovrane, evitando frammentazione.
Le aziende in grado di sviluppare e gestire tecnologie sovrano europee potranno poi essere un modello e un ponte tra Europa, Africa e Medio Oriente, diventando enabler di modelli di sovranità digitale vera per i paesi in via di sviluppo, in coerenza con il Piano Mattei e il Global Gateway.
Come nel passato si parlava di diplomazia dell'energia, in futuro si parlerà di diplomazia digitale, con accordi per scambi sicuri di dati tra blocchi geopolitici.

***Raccomandazione**: promuovere interconnessioni sicure e modelli federati, mantenendo però il controllo locale delle risorse critiche.*

L'agenda europea per il Cloud Sovrano

Come ho sostenuto nel contesto di Connect Europe, il Cloud Sovrano deve essere riconosciuto come infrastruttura critica, insieme a 5G, 6G e cavi sottomarini. Questo significa:

- mercato unico delle telecomunicazioni con regole armonizzate e meno frammentazione;
- classificazione chiara dei dati;
- partnership pubblico-private per creare piattaforme sovrane scalabili e competitive;
- investimenti mirati su Edge Cloud, data center a basso impatto ambientale e sicurezza;
- parità regolatoria con "same services, same rules" tra operatori europei e big tech globali;
- semplificazione normativa e riduzione degli oneri burocratici per accelerare la trasformazione digitale.

Se l'Europa vuole essere protagonista nella corsa tecnologica globale, deve garantire controllo, sicurezza, competitività e sostenibilità. Non è un'opzione, è una necessità industriale, tecnologica e geopolitica.

> ***Inaction is not an option: il momento di agire è adesso.***

Governance adattiva e compliance by design

Il quadro normativo europeo è in continua evoluzione: GDPR, Data Act, AI Act, NIS2, Digital Services Act, Cybersecurity Act e nuove iniziative come il Cloud and AI Development Act lo dimostrano. Un'infrastruttura sovrana deve essere dinamica, capace di adattarsi senza interruzioni ai nuovi requisiti. La compliance non deve essere un processo reattivo, ma integrata fin dalla progettazione.

***Raccomandazione**: adottare una governance flessibile, multilivello, che includa PA, imprese e organismi indipendenti di certificazione.*

Capitale umano e competenze

Senza capitale umano qualificato, nessun progetto di sovranità digitale può avere successo.

Servono Cloud architect, esperti di cybersecurity, crittografi, data governance officer. Per formare competenze cosi mirate e specialistiche, l'Italia deve creare academy nazionali e programmi congiunti università–imprese e frenare la fuga dei talenti, offrendo percorsi professionali attrattivi e valorizzando le competenze locali.

***Raccomandazione**: investire in capitale umano almeno quanto in infrastrutture tecnologiche.*

Integrazione con la strategia ESG

Il Cloud Sovrano del futuro non sarà solo sicuro, ma dovrà essere anche sostenibile.

I Data center che lo ospiteranno saranno alimentati da energie rinnovabili e certificate secondo metriche pubbliche di carbon footprint.
Adotteranno sistemi di free cooling e recupero del calore per usi industriali o residenziali e sistemi di crittografia low energy consuming (QKD) e non basati su soluzioni basate sulla mera espansione algoritmica, strutturalmente legata alla capacità energetica di sostenere il supercalcolo.

***Raccomandazione**: includere KPI ESG tra gli obiettivi strategici di ogni progetto, garantendo che la transizione digitale sia anche green.*

Visione di lungo termine per l'Italia (2035)

Se l'Italia saprà cogliere questa sfida, entro il 2035 potrà diventare:

- sede dello sviluppo digitale sicuro del Mediterraneo, punto di riferimento per Europa, Africa e Medio Oriente;
- un polo di attrazione per investimenti nei settori ad alta intensità di dati (AI, biotech, industria 4.0);
- un modello di governance pubblico-privato, esportabile in altri Paesi;
- un leader nella diplomazia dei dati, con corridoi sicuri di scambio digitale.

> *In un mondo in cui i dati sono la risorsa strategica più preziosa, il Cloud Sovrano è la raffineria nazionale: il luogo in cui trasformiamo i dati in valore economico, sociale e industriale, mantenendo sempre il controllo sulle nostre risorse più critiche.*

Conclusioni

Il Cloud Sovrano non è semplicemente un'infrastruttura digitale: è una scelta di politica industriale e una condizione di sicurezza nazionale.
In un mondo in cui i dati determinano la competitività economica, la capacità di innovare e persino l'equilibrio geopolitico, rinunciare al controllo delle informazioni significa rinunciare a una parte della propria sovranità.
L'Italia dispone di un vantaggio competitivo: il Polo Strategico Nazionale (PSN) è già operativo e conforme ai più alti standard di sicurezza. Ma questo non basta. Limitare il Cloud Sovrano alla sola Pubblica Amministrazione significherebbe proteggere una parte del patrimonio informativo nazionale, lasciando scoperte intere filiere industriali, settori critici e PMI che generano innovazione.

La direzione è chiara:

- modificare la normativa per una chiara classificazione dei dati e per estendere la protezione sovrana al settore privato strategico e alle filiere critiche;
- assicurare anche attraverso la connettività il controllo dei dati per evitare che gli stessi facciano il giro del mondo nel loro movimento dalla fonte di origine al Cloud;
- interconnettere le infrastrutture italiane con quelle europee, per costruire un fronte comune interoperabile e federato della sovranità digitale;
- investire nelle reti sovrane di supporto alle soluzioni Multi Cloud;
- investire nelle competenze perchè senza capitale umano specializzato, nessuna infrastruttura può essere davvero sovrana;
- integrare criteri ESG in ogni progetto, perché la sovranità del futuro sarà anche sostenibilità ambientale.

> *Il Cloud Sovrano è la raffineria dei dati: trasforma una materia prima inesauribile in valore economico, sociale e industriale, garantendo al contempo sicurezza e indipendenza.*

Per l'Italia, la sfida non è più capire se serva un Cloud Sovrano, ma decidere quanto velocemente e con quale ambizione costruirlo. È una responsabilità collettiva: istituzioni, imprese e cittadini devono riconoscere che la sovranità digitale non è un bene per pochi, ma un bene comune, che definisce il posto del Paese nel mondo di domani.
Non si può dimenticare che la sicurezza digitale di lungo periodo dipenderà anche dalla capacità di affrontare la sfida quantistica. La protezione dei dati richiede l'adozione di standard di cifratura resistenti al quantum computing, pena il rischio che informazioni sensibili custodite oggi vengano decifrate in futuro. Inserire il quantum come priorità strategica della sovranità digitale significa mettere al sicuro non solo l'attuale patrimonio informativo, ma anche quello delle generazioni future.

Lezioni trasversali per l'Italia

Dall'analisi di questi casi emergono alcune linee guida utili per il contesto italiano:

- giurisdizione locale del dato per evitare trasferimenti o sottomissioni dei dati a normative diverse;
- governance chiara perchè senza regole precise su chi gestisce cosa, la sovranità resta solo sulla carta;
- partnership pubblico-privato con i modelli vincenti che vedono la collaborazione stretta tra Stato e industria;
- approccio modulare per partire da settori strategici (energia, sanità, telecomunicazioni) e ampliare progressivamente;
- standard aperti per evitare isolamento tecnologico e garantire interoperabilità con partner europei;
- formazione e competenze perchè senza capitale umano specializzato, nessuna infrastruttura può essere davvero sovrana.

> *"Per l'Italia, con il Polo Strategico Nazionale già avviato, il passo successivo è estendere questo modello oltre la Pubblica Amministrazione, integrando best practice internazionali e rafforzando la filiera nazionale e facendo rispettare quanto già previsto dalle norme sul Perimetro di Sicurezza Nazionale Cibernetica, ampliandone man mano la portata anche ai soggetti NIS2."*

Pietro Labriola