ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

SCUOLA DI SCIENZE
Corso di Laurea in Informatica per il Management

Il progetto GAIA-X: Sovranità digitale tra stato e piattaforme

Tesi di Laurea in Storia e Politiche del Digitale

Relatore:
Chiar.mo Prof.
MATTIA FRAPPORTI

Presentata da:
DIEGO GALLINI

Sessione III
Anno Accademico 2024/2025

A chi mi ha accompagnato in questo percorso.

«Mi sei scoppiato dentro al cuore
All'improvviso, all'improvviso
Non so perché, non lo so perché
All'improvviso, all'improvviso»

— Mina

Abstract

Come possono gli Stati mantenere il controllo su dati e infrastrutture digitali in un contesto sempre più dominato da grandi piattaforme globali? Questa domanda è al centro del dibattito contemporaneo sulla sovranità digitale. Il presente lavoro analizza il rapporto tra istituzioni, piattaforme digitali e governance dei dati, concentrandosi in particolare sul progetto europeo GAIA-X come possibile strumento per rafforzare l'autonomia tecnologica dell'Europa e ridurre la dipendenza dai principali attori privati del mercato cloud.

Lo studio ricostruisce innanzitutto la trasformazione dell'ecosistema digitale e il ruolo delle piattaforme come infrastrutture centrali nell'economia dei dati. Successivamente vengono esaminate le principali strategie normative e politiche sviluppate dall'Unione Europea per rafforzare la governance dei dati e promuovere la sovranità digitale. Infine, viene approfondito il progetto GAIA-X, illustrandone obiettivi, principi architetturali, limiti, contraddizioni e in più in generale le dinamiche che veicolano il suo modello federativo volto a garantire la portabilità dei dati e la fiducia tra gli attori economici.

L'analisi evidenzia come la sovranità digitale richieda lo sviluppo di modelli tecnologici e infrastrutturali capaci di tradurre i principi europei in soluzioni operative. In tale prospettiva, iniziative come GAIA-X rappresentano un tentativo significativo di ridefinire le regole dell'ecosistema digitale europeo, promuovendo una reale autodeterminazione tecnologica e una gestione dei dati basata su valori e standard comuni.

Indice

Introduzione

Negli ultimi anni la crescente diffusione delle tecnologie digitali ha trasformato profondamente l'organizzazione economica, sociale e politica della società contemporanea. Tale mutamento poggia su infrastrutture complesse, quali sistemi cloud, piattaforme e grandi ecosistemi di dati, che sostengono il funzionamento di servizi pubblici e attività economiche. In questo contesto, i dati hanno assunto un ruolo centrale, divenendo una risorsa strategica per il funzionamento delle istituzioni pubbliche, per la competitività economica e per l'innovazione tecnologica.

Dietro al loro valore strategico si nascondono però una serie di questioni politiche e istituzionali. A differenza delle infrastrutture tradizionali, spesso localizzate e gestite direttamente dagli stati, e in ogni caso "territorializzabili" in qualche misura, molti sistemi contemporanei sono controllati da grandi imprese tecnologiche globali: multinazionali che forniscono servizi cloud, piattaforme e strumenti di gestione dei dati utilizzati anche dalle amministrazioni pubbliche. Questa trasformazione ha progressivamente posto il problema della dipendenza tecnologica da attori privati e della capacità delle istituzioni pubbliche di mantenere un controllo effettivo sui propri sistemi.

È in questo quadro che si spalanca il tema della sovranità digitale in tutte le sue sfumature e contraddizioni. In prima approssimazione, essa andrebbe intesa come l'effettiva capacità di uno stato di mantenere un presidio reale sulle infrastrutture digitali, sui dati e sulle tecnologie che sostengono il funzionamento della società. Tuttavia, tale prerogativa non può essere assunta in senso tradizionale: se in passato il controllo territoriale dei sistemi coincideva con la capacità effettiva di governarne l'utilizzo, nel contesto digitale questo non è più scontato. Servizi cloud e tecnologie sono distribuiti su scala globale e sviluppati da imprese multinazionali, rendendo dunque complesso il rapporto tra potere pubblico e attori privati. Per questo motivo, il tema della sovranità digitale ha acquisito negli ultimi anni una centralità teorica e concettuale importante sia a livello nazionale, sia a livello europeo e, in fondo, globale.

La sovranità, infatti, non può essere ridotta alla semplice proprietà delle infrastrutture o alla localizzazione fisica dei dati, ma deve essere interpretata come la capacità di definire e far rispettare le condizioni di utilizzo delle tecnologie, di stabilire standard tecnici e regole di

governance, e di garantire reali margini di autonomia nelle decisioni relative allo sviluppo dell'ecosistema.

La riflessione su questi temi è stata progressivamente sviluppata dall'Unione Europea, che ha individuato nella gestione dei dati uno degli elementi centrali per il futuro dell'economia continentale. Un punto di riferimento essenziale in questo dibattito è il report dell'European Parliamentary Research Service intitolato "Digital sovereignty for Europe", nel quale la sovranità digitale è descritta come la capacità dell'Europa di agire in modo autonomo nello spazio virtuale, combinando strumenti di tutela con politiche volte a promuovere innovazione e sviluppo tecnologico. In questa prospettiva, tale autonomia non implica un isolamento tecnologico, ma la possibilità di esercitare un'effettiva capacità di governo sulle condizioni di funzionamento dell'ambiente digitale.

Questa visione è stata integrata ulteriormente in alcuni documenti strategici della Commissione Europea, in particolare nella "Strategia Europea per i Dati", che individua nella costruzione di un mercato europeo dei dati uno degli obiettivi principali della trasformazione digitale. L'obiettivo principale del progetto è favorire la circolazione delle informazioni, garantendo però elevati standard di sicurezza, tutela dei diritti e rafforzamento della capacità di governare infrastrutture, standard e condizioni di utilizzo dei dati.

Dall'analisi delle politiche europee, tuttavia, emerge chiaramente come il tema non si esaurisca esclusivamente nella dimensione normativa. Negli ultimi anni, l'Unione ha costruito un articolato quadro regolatorio che comprende strumenti come il GDPR, il Data Governance Act, il Data Act e la direttiva NIS2. Questi pacchetti hanno rafforzato in modo significativo la protezione dei dati personali, la privacy e la sicurezza informatica, definendo un insieme di principi e garanzie giuridiche per la gestione delle informazioni nell'economia digitale.

Tuttavia, se sul piano giuridico il quadro europeo appare strutturato, va notato che questo può essere al contempo considerato il punto più avanzato in termini di efficacia diretta sul tema della sovranità digitale da parte dell'Europa, ma al contempo anche il suo limite più grande. Il dibattito, infatti, resta del tutto aperto per quanto riguarda le implicazioni operative e infrastrutturali che dovrebbero strutturare la sovranità digitale. È stato evidenziato in vari momenti come la solidità delle regole non elimini automaticamente le asimmetrie che

caratterizzano l'ecosistema tecnologico globale, specialmente laddove il controllo fisico dei sistemi critici rimane nelle mani di pochi attori privati e per di più extra-europei.

Il mercato globale del cloud computing risulta infatti fortemente concentrato nelle mani di pochi player internazionali, come Amazon Web Services, Microsoft e Google che da soli detengono i due terzi della capacità cloud a livello globale[1]. Questa concentrazione genera di fatto forme di dipendenza tecnologica che, pur in presenza di un quadro regolatorio articolato, continuano a sollevare interrogativi sulla capacità delle istituzioni pubbliche di mantenere un presidio concreto sulle architetture utilizzate per l'erogazione dei servizi e la gestione dei dati.

Alla luce di tali criticità è emersa l'esigenza di introdurre iniziative infrastrutturali e tecnologiche capaci di incidere direttamente sull'organizzazione dell'ecosistema. In questo contesto si colloca il progetto GAIA-X, iniziativa nata con l'obiettivo di sviluppare un'infrastruttura federata di dati e servizi cloud basata su standard comuni, interoperabilità e meccanismi di fiducia verificabili.

A differenza di altre iniziative orientate allo sviluppo di cloud proprietari, GAIA-X non si propone come un nuovo provider europeo centralizzato. Il suo obiettivo è piuttosto definire un insieme di regole tecniche, standard e meccanismi di interoperabilità capaci di federare infrastrutture esistenti e consentire a diversi provider di operare all'interno di un ecosistema comune.

Questa impostazione distingue GAIA-X da altre strategie adottate a livello nazionale, come il Polo Strategico Nazionale italiano, che persegue l'obiettivo di indipendenza tecnologica principalmente attraverso il controllo infrastrutturale e la localizzazione fisica dei servizi cloud. Mentre il modello del PSN si fonda su un'infrastruttura nazionale qualificata, GAIA-X propone un modello federato, nel quale l'autodeterminazione emerge dalla capacità di definire regole comuni e garantire interoperabilità tra più soggetti. Il confronto tra questi due modelli permette di riflettere sulle diverse strategie adottate per affrontare il problema della sovranità digitale. Da un lato emergono approcci basati sul rafforzamento delle infrastrutture nazionali e sul controllo diretto dei data center; dall'altro vengono delineati modelli

[1]F. Richter, *AWS Stays Ahead as Cloud Market Accelerates*, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/, ultimo accesso febbraio 2026.

federativi che puntano a ridefinire le regole di funzionamento del mercato dei dati attraverso standard e meccanismi di governance condivisa.

Alla luce di queste considerazioni, la presente tesi si propone proprio di analizzare il progetto GAIA-X come tentativo europeo di affrontare il nodo del governo dei dati all'interno di un ecosistema digitale globale caratterizzato da forti asimmetrie di potere tra stati e grandi piattaforme tecnologiche. L'obiettivo del lavoro è comprendere in che misura iniziative di questo tipo possano contribuire a rafforzare la capacità dell'Europa di governare l'evoluzione delle infrastrutture digitali e ridurre le dipendenze tecnologiche esistenti.

La struttura della tesi è articolata in tre capitoli: il primo capitolo analizza la trasformazione dell'ecosistema digitale e il ruolo di crescente centralità che assumono le piattaforme nell'organizzazione della società. Viene mostrato come i dati siano divenuti una risorsa strategica e come il controllo delle infrastrutture digitali influenzi gli equilibri di potere tra attori pubblici e privati.

Il secondo capitolo approfondisce il concetto di sovranità digitale nel contesto europeo, distinguendolo dalla semplice sicurezza informatica e analizzando le principali vulnerabilità che derivano dalla dipendenza da infrastrutture tecnologiche esterne. Viene inoltre brevemente esaminato il quadro normativo europeo e italiano, valutandone i limiti nel garantire un controllo effettivo sull'ecosistema digitale.

Il terzo capitolo è dedicato all'analisi del progetto GAIA-X, esaminandone il contesto di nascita, il modello di sovranità dei dati proposto e il funzionamento tecnico dell'architettura federata. Il capitolo si conclude con una valutazione critica dei risultati e dei limiti dell'iniziativa, interrogandosi sulla sua capacità di incidere sugli equilibri del mercato cloud europeo.

In termini di metodologia e fonti, la tesi si basa principalmente sull'analisi di documenti istituzionali, letteratura accademica e contributi provenienti da esperti del settore, con l'obiettivo di ricostruire il dibattito europeo sulla sovranità digitale e valutare il ruolo di GAIA-X in tale contesto.

Una prima categoria di fonti riguarda i documenti strategici delle istituzioni europee. In particolare, viene presa come riferimento la "Strategia europea per i dati"[2] pubblicata dalla

[2] Commissione Europea, *Una strategia europea per i dati*, in Comunicazioni della Commissione Europea, COM (2020) 66, 2020.

Commissione Europea nel 2020, documento che costituisce il fondamento della politica europea in materia di economia dei dati. All'interno di questa comunicazione viene delineato il progetto di costruzione di uno spazio europeo dei dati, finalizzato a favorire la circolazione e la condivisione delle informazioni tra attori pubblici e privati nel rispetto di standard comuni di sicurezza, trasparenza e tutela dei diritti fondamentali. L'analisi di tale documento consente di comprendere il quadro politico entro cui si inseriscono le iniziative europee dedicate alla governance dei dati e rappresenta il punto di partenza per interpretare la crescente attenzione dell'Unione verso il tema.

Accanto ai documenti della Commissione Europea è risultato rilevante anche il report dell'EPRS "Digital sovereignty for Europe"[3], uno dei contributi più citati nel dibattito sul tema. Questo studio fornisce una definizione articolata del concetto di sovranità digitale, interpretandolo come la capacità dell'Europa di agire in modo autonomo nello spazio digitale, sia attraverso strumenti di protezione delle infrastrutture sia mediante politiche volte a promuovere innovazione tecnologica e sviluppo industriale.

Un secondo gruppo di fonti riguarda il quadro normativo europeo relativo alla governance dei dati e alla cybersicurezza, composto da atti legislativi come il GDPR, il Data Governance Act, il Data Act e la direttiva NIS2. L'esame di queste normative è stato utilizzato principalmente per ricostruire il contesto regolatorio entro cui si sviluppa il dibattito sulla sovranità digitale e per comprendere in che modo l'Unione Europea abbia cercato di affrontare alcune delle vulnerabilità dell'ecosistema digitale attraverso strumenti giuridici. L'analisi normativa ha inoltre consentito di evidenziare la distinzione tra sicurezza informatica e sovranità digitale, mostrando come la prima riguardi prevalentemente la protezione dei sistemi e dei dati, mentre la seconda coinvolga anche aspetti più ampi legati al controllo delle infrastrutture digitali e alle condizioni di utilizzo delle tecnologie.

La parte principale dell'analisi si è concentrata sulla documentazione tecnica e programmatica relativa al progetto GAIA-X. In particolare, sono stati analizzati i principali documenti pubblicati da Gaia-X European Association for Data and Cloud AISBL, tra cui l'Architecture Document, il Trust Framework e i documenti dedicati ai criteri di conformità e ai meccanismi di certificazione dell'ecosistema. Questi materiali permettono di comprendere in modo approfondito il funzionamento tecnico dell'architettura e il modello di governance dei dati

[3] T. Madiega, *Digital sovereignty for Europe*, European Parliamentary Research Service (EPRS), Briefing Paper, PE 651.992, 2020.

che essa propone. L'analisi della documentazione architetturale è stata fondamentale per ricostruire i principali componenti dell'ecosistema GAIA-X, come il sistema delle Self-Descriptions, i servizi federativi e i meccanismi di verifica basati su credenziali, che costituiscono gli elementi attraverso cui il progetto tenta di tradurre il concetto di sovranità dei dati in una configurazione operativa.

La ricerca ha inoltre preso in considerazione alcuni documenti istituzionali pubblicati dai governi nazionali che hanno promosso l'iniziativa, per comprendere il contesto politico e industriale in cui è nato il progetto, in particolare dai ministeri dell'economia di Germania e Francia. Questi documenti consentono di ricostruire le motivazioni politiche alla base della nascita di GAIA-X e il ruolo che l'iniziativa intende svolgere all'interno delle strategie europee dedicate all'autonomia tecnologica e allo sviluppo dell'economia dei dati. L'analisi di tali fonti ha permesso di evidenziare come il progetto sia stato concepito non soltanto come iniziativa tecnica, ma anche come parte di una più ampia strategia industriale europea volta a rafforzare la capacità del continente di competere nel settore delle infrastrutture digitali.

Accanto all'analisi documentale, il lavoro è stato integrato da alcune interviste condotte con professionisti che operano direttamente nel settore delle infrastrutture digitali e della governance dei dati in ambito di amministrazioni pubbliche.

In particolare, è stata realizzata un'intervista a Paolo Fontechiari[4], Responsabile S.O. Infrastrutture Tecnologiche e Telecomunicazioni del Comune di Parma. Questo contributo ha permesso di analizzare il tema della sovranità digitale dal punto di vista delle amministrazioni pubbliche, mettendo in luce le principali criticità legate alla gestione dei servizi cloud, alla dipendenza tecnologica dai grandi provider e alle difficoltà tecniche e organizzative che possono emergere nell'adozione di nuove infrastrutture digitali. L'intervista ha inoltre consentito di approfondire il caso del Comune di Parma e il tentativo di utilizzare infrastrutture di controllo pubblico, come la rete Lepida o It.City, per sviluppare soluzioni alternative nella gestione dei servizi digitali e dei dati, evidenziando le opportunità ma anche i limiti operativi di queste iniziative.

[4] Intervista realizzata dall'autore in data 29 gennaio 2026 a Paolo Fontechiari, Responsabile della S.O. Infrastrutture Tecnologiche e Telecomunicazioni del Comune di Parma. Trascrizione integrale disponibile in Appendice 1.

Una seconda intervista è stata condotta con l'avvocato Francesco Montesi[5], consulente legale in privacy e data protection. Il suo contributo è stato fondamentale per comprendere come il quadro normativo europeo relativo alla protezione dei dati e alla cybersicurezza venga interpretato e applicato. Questa prospettiva ha permesso di approfondire il rapporto tra regolazione giuridica e gestione operativa dei dati, evidenziando alcune delle difficoltà che emergono quando le normative vengono implementate in contesti organizzativi complessi.

Infine, è stata realizzata un'intervista a Leonardo Lorenzetto[6], Presale Engineer & Solution Architect di un'azienda operante nel settore sicurezza e cloud per la Pubblica Amministrazione e le imprese. Questa testimonianza ha consentito di approfondire gli aspetti tecnici e progettuali legati alla realizzazione di architetture cloud e di comprendere come modelli federati come quello proposto da GAIA-X vengano percepiti e valutati da operatori che lavorano direttamente nello sviluppo e nell'integrazione di infrastrutture digitali.

Nel loro insieme, queste fonti hanno consentito di analizzare il progetto GAIA-X non soltanto come iniziativa tecnologica, ma come parte di un più ampio tentativo di ridefinire il rapporto tra potere pubblico e grandi piattaforme globali. L'elaborato si propone quindi di mostrare come tale modello rappresenti uno dei tentativi più rilevanti sviluppati in Europa per affrontare il problema della sovranità digitale. Attraverso l'integrazione tra documenti istituzionali, letteratura accademica e testimonianze dirette, il lavoro intende mettere in luce potenzialità e limiti di GAIA-X, mantenendo un'attenzione costante alle implicazioni politiche e istituzionali legate alla gestione degli asset tecnologici e alla governance dei dati.

[5] Intervista realizzata dall'autore in data 22 febbraio 2026 a Francesco Montesi, consulente legale in privacy e data protection. Trascrizione integrale disponibile in Appendice 2.
[6] Intervista realizzata dall'autore in data 27 febbraio 2026 a Leonardo Lorenzetto, Presale Engineer & Solution Architect di un'azienda operante nel settore cloud per la Pubblica Amministrazione. Trascrizione integrale disponibile in Appendice 3.

Capitolo 1

Piattaforme come nuove infrastrutture

Introduzione

Negli ultimi decenni, le modalità di comunicazione, produzione e organizzazione della vita sociale sono state profondamente trasformate dall'innovazione. Il mondo digitale, che si presentava inizialmente come aperto, decentralizzato e orientato alla libera circolazione delle informazioni è profondamente cambiato, tramutandosi in un sistema chiuso e dominato da pochi attori privati. Per comprendere a pieno questa trasformazione è necessario analizzare sia l'evoluzione tecnica, ma anche le implicazioni politiche, economiche e sociali che ne derivano. Infatti, le piattaforme digitali, oggi centrali nella vita di individui e istituzioni, non sono più solo strumenti tecnologici, ma svolgono un ruolo strutturale nell'organizzazione dello spazio digitale, incidendo sull'esercizio del potere, sulle interazioni e sulle condizioni di accesso alle informazioni. In questo capitolo verrà analizzato il processo attraverso il quale le piattaforme si sono affermate come nuove infrastrutture del digitale. A tal fine, nella prima parte si ripercorrerà l'evoluzione storica della rete, e il passaggio da un'architettura aperta a un modello centralizzato. Successivamente, le piattaforme verranno analizzate come infrastrutture tecnologiche e politiche, capaci di esercitare forme di potere attraverso la loro architettura. In seguito, verrà approfondito il ruolo e il valore dei dati nel capitalismo delle piattaforme, con un focus sul capitalismo della sorveglianza e il tema dell'estrazione del valore. Infine, verrà introdotto il tema del rapporto stato-piattaforme, analizzando i rischi di questa dipendenza, anche grazie al caso studio del Comune di Parma. Questo percorso risulta fondamentale per la tesi, poiché chiarisce come il controllo delle infrastrutture digitali e dei dati costituisca oggi una delle principali fonti di potere, ponendo nuove sfide in termini di autonomia, regolazione e sovranità.

1.1 Passaggio da web aperto, a piattaforme ed ecosistemi

In questa prima parte del capitolo sarà possibile comprendere come le piattaforme siano diventate le nuove infrastrutture del digitale. A questo fine è opportuno anzitutto ripercorrere l'evoluzione storica della rete e del web. In questo quadro, il primo progetto di una rete per

collegare un insieme di calcolatori risale agli anni ’60. Sviluppata in ambito militare e di ricerca, la rete Arpanet permetteva lo scambio di informazioni tra i vari laboratori dei centri di ricerca del Dipartimento della Difesa degli Stati Uniti. In questa fase iniziale, tuttavia, le reti non costituivano ancora un sistema unitario e interoperabile. Le comunicazioni avvenivano all’interno di reti chiuse e proprietarie, basate su standard non compatibili tra loro, ma dipendenti da singoli fornitori e sviluppate da aziende come IBM, che promosse la Systems Network Architecture (SNA). Un passaggio decisivo avvenne negli anni Settanta, con lo sviluppo del protocollo TCP/IP, che rese possibile l’interconnessione tra reti eterogenee. Il momento di svolta si colloca nel 1983, quando TCP/IP viene adottato ufficialmente come protocollo standard di Arpanet, sostituendo i precedenti protocolli proprietari. A differenza dei sistemi precedenti, questo protocollo si basa su uno standard aperto e documentato, che favorisce l’interoperabilità e un’architettura decentralizzata. Su questa architettura aperta e decentralizzata nasce, alla fine degli anni Ottanta, il World Wide Web, dall’idea del ricercatore inglese del CERN Tim Berners-Lee. L’obiettivo originale del web era favorire la libera circolazione delle informazioni e l’interoperabilità tra sistemi eterogenei. A tal fine, l’architettura iniziale era basata su protocolli e linguaggi aperti, come HTTP per lo scambio di dati e risorse e HTML per la creazione delle pagine. In questa fase le comunicazioni non richiedevano la mediazione di piattaforme centralizzate, ma si basavano su standard condivisi che consentivano a una pluralità di attori di produrre e accedere ai contenuti. Come scrive Barners-Lee, infatti, il web è stato progettato intenzionalmente come un’infrastruttura priva di punti centrali di controllo, sia per ragioni filosofiche che tecniche, poiché qualsiasi forma di centralizzazione avrebbe impedito la crescita del sistema.

> I had designed the Web so there should be no centralized place where someone would have to “register” a new server, or get approval of its contents. Anybody could build a server and put anything on it. Philosophically, if the Web was to be a universal resource, it had to be able to grow in an unlimited way. Technically, if there was any centralized point of control, it would rapidly become a bottleneck that restricted the Web's growth, and the Web would never scale up. Its being “out of control” was very important.[7]

Questo modello implicava una chiara separazione tra infrastruttura e contenuti. La rete forniva il livello base per le comunicazioni, mentre tutti i contenuti, informazioni e servizi venivano sviluppati in modo indipendente, riducendo il rischio di concentrazione del potere.

[7] T. Berners-Lee (2017), *Weaving The Web. The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*, New York, Harper Business, p. 99.

Infatti, come osserva Lawrence Lessig[8], giurista e avvocato statunitense, studioso del rapporto tra diritto, tecnologia e internet, l'architettura del web incorporava implicitamente una visione politica basata sulla decentralizzazione, nella quale il potere non era concertato tra soggetti privati, ma nemmeno in capo allo stato, ma distribuito tra molteplici attori.

Dagli anni Duemila, tuttavia, questo modello ha iniziato a mostrare dei limiti strutturali. L'aumento esponenziale di produzione e utilizzo di dati e la crescente complessità dei servizi digitali ha favorito l'emergere di nuovi attori su scala globale. In questo contesto si affermano le piattaforme digitali, che trasformano il modello iniziale in un ecosistema completamente diverso, caratterizzato da enti privati che si propongono come intermediari in grado di coordinare grandi quantità di utenti, dati e risorse, rispondendo ai problemi di scalabilità, coordinamento e gestione delle complessità. Il passaggio da web aperto a piattaforme non rappresenta quindi una semplice evoluzione tecnologica, ma una completa trasformazione dell'architettura dello spazio digitale.

Come osserva Nick Srnicek, giornalista e docente di economia digitale al King's College di Londra, le piattaforme possono essere viste come

> Infrastrutture digitali che rendono possibile l'interazione tra due o più gruppi. Le piattaforme si posizionano dunque come intermediari che associano diversi gruppi di utenti: clienti, pubblicitari, fornitori di servizi, produttori, fornitori, e perfino oggetti fisici[9].

In questa prospettiva, le piattaforme, non sono delle semplici imprese digitali, ma costituiscono delle infrastrutture economiche, paragonabili a reti energetiche o sistemi di trasporto, che stanno alla base per l'organizzazione di attività produttive e sociali su larga scala. Queste non si limitano ad offrire solo servizi, ma creano ambienti chiusi con regole d'accesso e condizioni. In questo senso, esse operano come nuovi nodi infrastrutturali del capitalismo digitale, diventando il principale modello economico e producendo profitto attraverso lo sfruttamento dei dati.

Dalla nostra analisi è possibile notare come il concetto iniziale di web aperto, basato su standard interoperabili, sia completamente mutato. Questa trasformazione si manifesta in modo particolarmente evidente nella nascita di ecosistemi digitali. Con questo termine

[8] L. Lessig (1999), *Code and Other Laws of Cyberspace*, New York, Basic Books, pp. 97-99.
[9] N. Srnicek (2017), *Capitalismo Digitale. Google, Facebook, Amazon e La Nuova Economia Del Web*, Roma, Luiss, p.57.

intendiamo insiemi chiusi e integrati di servizi, applicazioni e infrastrutture gestiti completamente da piattaforme private, che operano secondo regole tecniche e contrattuali definite internamente. Le piattaforme, infatti, comprendono un insieme di applicazioni e servizi in un unico ambiente chiuso, con l'obiettivo di incentivare l'utente a utilizzare una gamma sempre più ampia di servizi interconnessi, riducendo la necessità di ricorrere a soluzioni alternative. La logica dei provider è quella di trattenere dati, utenti e le loro attività, cercando di generare valore da questi, come ben spiega Srnicek nel corso del suo testo. Per questo introducono meccanismi di dipendenza che comportano costi elevati per utenti e istituzioni, ed elevata difficoltà di uscita da essi, in un meccanismo definito di lock-in. Tali meccanismi possono essere di natura tecnica, come l'uso di formati, protocolli e standard proprietari, ma anche di natura cognitiva, legata alle abitudini degli utenti. Un esempio di questo modello è rappresentato da Amazon, che utilizza algoritmi proprietari, basati su criteri non trasparenti di ranking e promozione per organizzare la visibilità dei prodotti e strutturare il mercato. A cui si accompagnano a meccanismi cognitivi degli utenti, che delegano alla piattaforma la valutazione dei prodotti e la loro rilevanza.

A partire da questi elementi, è importante sottolineare come le piattaforme vadano comprese come vere e proprie infrastrutture socio-tecniche, che riorganizzano lo spazio economico e politico, ridefinendo i rapporti tra capitale, lavoro e stato. Pur essendo imprese private, svolgono funzioni di regolazione dell'accesso all'informazione, sulla visibilità dei contenuti e sulla possibilità di partecipazione alla vita pubblica. In questa direzione, Jean Christophe Plantin, professore di Media and Communication alla London School of Economics, portando l'esempio di Facebook, descrive come le piattaforme si stiano espandendo e integrando nella nostra vita, assumendo un numero crescente di funzioni.

> As an infrastructure, Facebook is progressively expanding and embedding itself in our daily existence, taking over more and more functions formerly provided by other, less restrictive means.[10]

Approfondendo questa dinamica, Plantin propone di analizzare le piattaforme attraverso un quadro teorico che mette in dialogo gli *infrastructure studies* e i *platform studies*. Secondo l'autore, solo integrando questi due approcci è possibile comprendere adeguatamente la

[10] J. Plantin, *Infrastructure studies meet platform studies in the age of Google and Facebook*, in Sage Journals, New Media & Society, p.12.

natura dei grandi attori digitali, come Facebook, che non possono essere interpretati né come semplici imprese tecnologiche né come semplici infrastrutture tecniche.

Gli *infrastructure studies* si concentrano sull'analisi di sistemi socio-tecnici essenziali, come reti elettriche o di trasporto, ampiamente integrati e condivisi nella vita quotidiana. Tali infrastrutture sono caratterizzate da proprietà come l'affidabilità, la durata nel tempo, l'onnipresenza e una tendenza all'invisibilità. Inoltre, proprio per il loro ruolo strutturale, sono considerate beni di interesse pubblico, soggetti a forme di regolazione statale.

I *platform studies,* invece, si concentrano sullo studio delle piattaforme digitali come ambienti programmabili, progettati per connettere attori differenti e favorire la produzione di servizi e contenuti. In questa prospettiva, l'analisi si sposta sia sulle funzionalità tecniche, sulle interfacce e sulle API, sia sulle modalità con cui le piattaforme esercitano forme di controllo e di orientamento degli individui. Infatti, la loro architettura riflette e incorpora specifici obiettivi economici e di estrazione del valore.

Il contributo di Plantin consente di comprendere come le piattaforme e le infrastrutture tendano oggi a sovrapporsi e trasformarsi reciprocamente. A questo proposito si parla di un duplice processo: da un lato l'infrastructuralization of platforms, dall'altro la platformization of infrastructures. Con il primo termine intendiamo il processo attraverso cui le piattaforme, nate come fornitrici di servizi, assumano le caratteristiche tipiche delle infrastrutture. Invece con il secondo termine si fa riferimento alla riorganizzazione di infrastrutture esistenti secondo le logiche delle piattaforme. Infatti, secondo l'autore:

> We argue that the rise of digital technologies, in a neoliberal, political, and economic climate, has simultaneously facilitated a "platformization" of infrastructures and an "infrastructuralization" of platforms.[11]

Uno dei meccanismi attraverso cui si realizza questa trasformazione è rappresentato dalle API, che Plantin interpreta come gateways infrastrutturali. Ovvero strumenti che consentono l'interconnessione tra i diversi sistemi, ma che al contempo rafforzano il controllo della piattaforma sull'ecosistema complessivo. L'interoperabilità, dunque, non assume la forma di uno standard condiviso, ma un'apertura selettiva governata dal soggetto privato.

Questa configurazione genera tensione tra interesse pubblico e logiche proprietarie. Infatti, come viene evidenziato, il carattere politico di questo processo risiede nella capacità delle

[11] Ivi, p.6.

piattaforme di esercitare forme di governo attraverso l'architettura tecnica, contribuendo a modificare i rapporti nello spazio digitale.

Alla luce di queste considerazioni, il passaggio da web aperto alle piattaforme può essere interpretato come una trasformazione profonda dello spazio digitale: una sua "infrastrutturazione", nella quale si favoriscono meccanismi tecnici di selezione e organizzazione rispetto alla neutralità e allo spazio aperto. A differenza della concezione originale del web, caratterizzato da una separazione tra tecnologia e potere, tali meccanismi non sono definiti da standard condivisi, ma incorporati in infrastrutture proprietarie.

Questa trasformazione assume particolare rilevanza per le istituzioni pubbliche, poiché introduce nuove forme di dipendenza strutturale verso soggetti privati, che coinvolgono non solo utenti e imprese, ma soprattutto stati. Il potere delle piattaforme non si limita quindi solo alla dimensione economica, ma investe la capacità di modellare l'ambiente digitale stesso, ponendo nuove questioni in termini di controllo, dipendenza e sovranità.

1.2 Le piattaforme come infrastrutture tecnologiche e politiche

Alla luce di questa trasformazione del web, le piattaforme digitali assumono una crescente centralità, e possono essere comprese non soltanto come imprese economiche, ma come vere e proprie infrastrutture tecnologiche e politiche. In quanto tali, si affermano come architettura dominante dello spazio digitale, assumendo un ruolo che va oltre la fornitura di servizi online. In questa prospettiva, possono essere comprese come ambienti complessi, nei quali tecnologia, potere e organizzazione si intrecciano, definendo così le condizioni entro cui si svolgono interazioni economiche, comunicative e sociali. Questa lettura ci fa comprendere come il potere delle piattaforme derivi specialmente dalla loro capacità di organizzare e governare ambienti digitali, portando l'analisi da un piano economico a quello politico.

Infatti, la loro centralità è costruita soprattutto a partire dalla grande capacità di raccolta ed elaborazione di grandi quantità di dati, risorsa principale dell'economia digitale, nella sua interpretazione di base del "capitalismo della sorveglianza", per riprendere una nota formula di Shoshana Zuboff[12], sociologa americana, professoressa e business analyst di Harvard. È proprio questa funzione e capacità che offre alle piattaforme la forza di imporsi come infrastruttura fondamentale per il funzionamento della vita sociale *tout court.* Non sono più

[12] S. Zuboff (2019), *Il capitalismo della sorveglianza*, Roma, Luiss.

soltanto – ammesso che lo siano mai state – mezzi utili al mondo digitale. Al contrario, sono modelli che si impongono nello spazio analogico dettando ritmi e dinamiche della vita politica e sociale.

In questo senso, va posta una certa attenzione a cosa si intende qui con il concetto di infrastruttura. Esso non può però essere ridotto a una dimensione puramente tecnica. Le infrastrutture «vanno annoverate piuttosto tra le attrici (principali) della governamentalità contemporanea»[13], in quanto regolano flussi e contribuiscono alla produzione di forme di organizzazione sociale. Sono strumenti politici, perché agiscono a monte dei comportamenti individuali e collettivi, definendo gli unici contesti in cui pratiche economiche, informative, sociali e politiche diventano possibili.

A differenza delle infrastrutture tradizionali, come reti energetiche o di trasporto, solitamente di proprietà pubblica, le piattaforme digitali sono gestite di fatto nella sua totalità da attori privati. Tuttavia, nonostante questa differenza, svolgono funzioni analoghe alle infrastrutture tradizionali, indispensabili per il funzionamento della società. Negli Stati Uniti queste piattaforme vengono definite con l'acronimo FAANG cioè Facebook, Apple, Amazon, Netflix e Google. Come osserva Guido Strazi[14], segretario generale dell'Antitrust, queste società hanno accumulato un tale potere economico e politico da poter essere descritte come veri e propri 'stati paralleli', capaci di operare su scala mondiale, influenzare mercati e crescere senza un adeguato quadro regolatorio.

Il potere delle piattaforme va inoltre inteso nella sua capacità di manifestarsi nella fase di intermediazione di relazioni. Esse non si limitano solamente a mettere in contatto soggetti diversi, ma definiscono le modalità in cui le comunicazioni possono avvenire. In particolare, stabiliscono regole di accesso, criteri, procedure e standard tecnici che condizionano gli utenti. Tale funzione di intermediazione non è neutrale, dal punto di vista tecnologico questo potere si esercita attraverso l'architettura dei sistemi informatici. Lo spazio digitale viene gestito tramite algoritmi, interfacce, sistemi di ranking e meccanismi di moderazione. Come affermato efficacemente da Lessig, «Code is law»[15], ovvero la funzione normativa viene svolta dal codice, perché definisce ciò che è consentito e visibile in un ambiente digitale. Il

[13]M. Frapporti, *Il potere delle piattaforme come infrastrutture. Tecnica, estetica, egemonia*, in Scienza & Politica, 2024.
[14] G. Strazi, *Il potere delle piattaforme digitali tra economia e politica*, https://eticaeconomia.it/il-potere-delle-piattaforme-digitali-tra-economia-e-politica/, ultimo accesso gennaio 2026.
[15] L. Lessig (1999), *Code and Other Laws of Cyberspace*, New York, Basic Books, pp. 13-37.

problema è quindi che questa funzione normativa non è il risultato di decisioni pubbliche, ma di scelte progettuali interne alle organizzazioni.

Gli algoritmi sono in effetti centrali nell'analisi delle piattaforme. Essi operano attraverso meccanismi di selezione e prioritizzazione, in virtù dei quali l'ordine dei contenuti o la loro visibilità non sono spontanei, ma frutto di decisioni del sistema. In questo modo viene applicata una forma di regolazione indiretta sulle decisioni e comportamenti assunti dagli utenti, questi non vengono obbligati a conformarsi, ma vengono influenzate le scelte disponibili e le traiettorie d'azione.

In questa prospettiva risulta ancora una volta particolarmente utile il contributo di Shoshana Zuboff per comprendere la natura del potere esercitato dalle piattaforme, al di là della dimensione economica. L'autrice introduce infatti il concetto di instrumentarian power, per descrivere una forma di potere che non si basa sulla coercizione o sull'ideologia, ma sulla capacità di orientare i comportamenti, modificando le condizioni entro cui gli individui prendono decisioni, rendendo così alcune azioni più probabili di altre. Come afferma Zuboff: «questo potere che definisco strumentalizzante ha il compito di strutturare e strumentalizzare il comportamento al fine di modificarlo, predirlo, monetizzarlo e controllarlo».[16]

Ne deriva una configurazione del potere politico esercitato profondamente atipica e non tradizionale: non si svolge infatti tramite istituzioni o norme giuridiche, ma attraverso la costruzione e gestione di spazi digitali in cui si svolgono le interazioni sociali. Questo potere non risiede nella sua capacità di imporre decisioni o obblighi, bensì nel creare le condizioni in cui tali decisioni diventano possibili. Le piattaforme, dunque, non governano al posto dello stato in maniera diretta, ma intervengono ad un livello inferiore, sull'architettura stessa dell'agire sociale. Per questa ragione, tale forma si differenzia dalle classiche modalità di esercizio di potere, basate sulla sovranità territoriale o sulla coercizione. Le piattaforme non rivendicano formalmente una funzione di governo, tuttavia condizionano indirettamente l'ambito di intervento del potere pubblico, incidendo sulle condizioni su cui si sviluppano pratiche sociali, economiche e politiche.

[16] S. Zuboff (2019), *Il capitalismo della sorveglianza*, Roma, Luiss, p.409.

1.3 Il potere dei dati e il capitalismo delle piattaforme

Come abbiamo visto, i dati sono uno dei principali motivi che permettono alle piattaforme di possedere potere. La capacità di raccogliere, elaborare e analizzare enormi quantità di informazioni rappresenta la base su cui si fonda il loro modello economico, ma anche una forma di potere politico. Infatti, i dati consentono di conoscere pienamente individui, gruppi sociali e dinamiche collettive, sono una risorsa strategica capace di influenzare comportamenti e decisioni.

Questa centralità dei dati emerge con particolare evidenza osservando le diverse analisi del settore basate su report IDC e Seagate, secondo cui il volume globale di dati generati annualmente è cresciuto in modo esponenziale: da circa 15,5 zettabyte del 2015 si è passati a 181 zettabyte nel 2025, con una stima di 221 zettabyte nel 2026, con un aumento annuale medio di circa 27%.[17] Una parte rilevante di questi dati viene gestita da un numero ristretto di piattaforme digitali, che operano come nodi centrali delle infrastrutture. Nello specifico, e fuor di metafora, a governare il sistema di immagazzinamento ed elaborazione algoritmica dei dati sono Amazon con la branca di Amazon Web Service, Microsoft con Azure e Google con Google Cloud Provider, i quali controllano circa i due terzi della capacità cloud globale: una cifra impressionante[18].

Le piattaforme, tuttavia, non si limitano a raccogliere dati in modo neutrale. Al contrario, gli ambienti digitali sono costruiti infatti per massimizzare la produzione di informazioni. Ogni interazione, clic, spostamento, tempo di permanenza viene analizzato per ricavarne valore. In questo senso, è noto che Google elabora oltre cinque trilioni di ricerche ogni anno[19], Meta aggrega enormi quantità di dati comportamentali per la profilazione e la previsione, Amazon gestisce set di dati relativi alle abitudini di consumo e alle preferenze degli utenti, con l'unico obiettivo di prevedere i comportamenti e orientare le scelte per motivi economici.

Come accennato precedentemente, questa modalità viene definita da Zuboff con il concetto di "Capitalismo della sorveglianza". Ovvero un sistema di accumulazione sistematica di dati comportamentali degli utenti, fondato sull'appropriazione di ogni elemento dell'esperienza

[17] N. Kumar, *Big Data Statistics 2026 (Growth, Trends & Market Size)*, https://www.demandsage.com/big-data-statistics/, ultimo accesso gennaio 2026.
[18]F. Richter, *AWS Stays Ahead as Cloud Market Accelerates*, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/, ultimo accesso febbraio 2026.
[19] Google, *AI, personalization, and the future of shopping*, https://blog.google/products/ads-commerce/ai-personalization-and-the-future-of-shopping/, ultimo accesso gennaio 2026.

umana. La vita quotidiana degli individui viene trasformata in materia prima, senza che questi ne abbiano piena consapevolezza o controllo. L'autrice lo definisce «intimamente parassitico e autoreferenziale. Rimanda alla vecchia immagine di Karl Marx del capitalismo come un vampiro che si ciba di lavoro. C'è però una svolta inattesa. Il capitalismo della sorveglianza non si ciba di lavoro, ma di ogni aspetto della vita umana».[20]

È possibile approfondire questo tema seguendo l'argomentazione data da Zuboff, secondo cui il capitalismo della sorveglianza rappresenta una nuova forma storica di capitalismo, distinto sia da quello industriale che da quello dell'informazione. La sua specificità non risiede unicamente nell'uso intensivo delle tecnologie digitali, ma nella ridefinizione del rapporto tra conoscenza, potere ed esperienza umana. In questo modello, la conoscenza è orientata alla previsione e all'orientamento dei comportamenti, e non solo alla comprensione dei fenomeni sociali.

Il potere delle piattaforme deriva quindi dalla capacità di convertire la conoscenza in uno strumento di intervento, contribuendo a influenzare le condizioni entro cui gli individui prendono decisioni. Questa è una forma di potere che opera a monte delle scelte, intervenendo sulle possibilità di azione piuttosto che imponendo obblighi diretti. Viene così sottolineato come questo potere non assume forme coercitive tradizionali, ma agisca tramite processi di progressivo adattamento e normalizzazione. Le piattaforme, sfruttando la loro posizione di superiorità, costruiscono ambienti in cui indirizzano gli utenti a compiere determinate scelte, mettendo in discussione l'autonomia individuale degli individui. Questo tipo di potere si concretizza soprattutto a livello infrastrutturale, dove le piattaforme hanno la possibilità di entrare nella vita dei cittadini, e acquisire così la possibilità di "datificare" tutti i comportamenti. Secondo Zuboff, «nel capitalismo della sorveglianza, i mezzi di produzione sono al servizio dei mezzi di modifica del comportamento»[21]. Per questo motivo esiste un potere strumentalizzante, che ha l'obiettivo di «di strutturare e strumentalizzare il comportamento al fine di modificarlo, predirlo, monetizzarlo e controllarlo»[22]

È proprio su queste basi teoriche si fonda il meccanismo economico individuato da Zuboff, legato alla trasformazione sistematica dell'esperienza umana in risorsa. L'autrice scrive infatti che «il capitalismo della sorveglianza si appropria della natura umana per produrre le

[20] S. Zuboff (2019), *Il capitalismo della sorveglianza*, Roma, Luiss, p.20.
[21] Ivi, p.470.
[22] Ivi, p.471.

proprie merci»[23]. Per chiarire come questo processo diventi operativo è necessario introdurre il tema di surplus comportamentale, che consente di comprendere in che modo l'esperienza degli utenti venga trasformata in valore economico e potere predittivo.

Il surplus comportamentale viene definito come l'estrazione di una quantità eccessiva di informazioni, non direttamente necessarie al funzionamento di un servizio, utilizzate dalle piattaforme per fini ulteriori. Questo surplus non viene utilizzato in modo "positivo", magari per il miglioramento del servizio, ma per sviluppare modelli predittivi e anticipare comportamenti futuri. Qui risiede il valore economico e politico di questo modello. È importante sottolineare come tale eccesso informativo non è il risultato inevitabile della digitalizzazione, ma una scelta progettuale e organizzativa. Le piattaforme costruiscono appositamente ambienti orientati alla massimizzazione della produzione dati, trasformando le informazioni degli utenti in una risorsa da estrarre. Di conseguenza il capitalismo della sorveglianza nasce come necessità tecnica, ma come modello economico fondato sull'estrazione sistematica dei dati.

Il rapporto tra piattaforme, utenti, imprese e istituzioni pubbliche risulta così strutturalmente asimmetrico, producendo una nuova forma di disuguaglianza del potere. Questo poiché pochi attori globali concentrano enormi quantità di dati consolidando un vantaggio difficilmente replicabile e rafforzando la propria posizione dominante.

Un caso emblematico di questo meccanismo è rappresentato dallo scandalo Cambridge Analytica, che ha coinvolto Facebook e l'utilizzo dei dati personali di circa 87 milioni di utenti[24], e ha reso evidente l'incidere sulla politica di questa dimensione. Il caso riguarda la raccolta di dati da parte dell'applicazione di test psicologici chiamata "This is your digital life" sviluppata dallo psicologo americano Aleksandr Kogan. L'applicazione, in conformità alle policy di Facebook allora vigenti, aveva accesso non solo alle informazioni degli utenti che si sottoponevano volontariamente ai test, ma anche a quelle dei loro contatti, senza che queste avessero espresso un consenso diretto e informato. Tali dati raccolti vennero poi utilizzati da Cambridge Analytica, società di consulenza politica britannica, per costruire profili psicometrici dettagliati, basati su tratti comportamentali e orientamenti politici. Questi profili furono impiegati per attività di micro-targeting politico, attraverso l'invio di messaggi a

[23] Ivi, p.112.
[24] O. Solon, *Facebook says Cambridge Analytica may have gained 37m more users' data*, in The Guardian, 2018.

specifici gruppi di elettori, con l'obiettivo di influenzare le scelte durante alcune campagne elettorali, in particolare per la Brexit nel 2018 e per le presidenziali negli Stati Uniti nel 2016. Questo scandalo ha reso evidente di come il controllo delle piattaforme sulle infrastrutture digitali permetta di esercitare grande influenza sui processi democratici, mettendo in discussione la neutralità tecnologica del web.

Le piattaforme conoscono gli utenti in maniera così dettagliata perché sono in grado di integrare dati da fonti eterogenee. Non si tratta solo di informazioni generate online, ma anche di dati raccolti tramite dispositivi come sensori, assistenti vocali e sistemi gps. Le stime indicano che a fine 2025 risultano attivi circa 21,1 miliardi di dispositivi IoT connessi, e potranno raggiungere i 39 miliardi entro il 2030[25], ciascuno dei quali contribuisce a generare flussi continui di dati.

Anche dal punto di vista economico le posizioni dominanti vengono rafforzate dal controllo dei dati. Le piattaforme beneficiano di economie di scala e di rete: più utenti utilizzano un servizio, più dati vengono raccolti, più accurati diventano i modelli predittivi e più i servizi che offrono diventano attrattivi. Viene creato così un circolo vizioso, che rende difficile l'ingresso di nuovi concorrenti e consolida il potere dei pochi attori presenti. Infatti, secondo il Financial Times[26] le otto maggiori società (Apple, Microsoft, Amazon…), dell'S&P 500, principale indice azionario americano, appartengono al settore tecnologico, evidenziando un'elevata concentrazione di valore nelle imprese tech.

Tuttavia, il problema centrale non è solo economico. Il capitalismo delle piattaforme introduce una trasformazione profonda nei rapporti tra potere, conoscenza e libertà individuale. L'autonomia degli individui e la trasparenza dei processi decisionali è sempre più messa in discussione, rendendo sempre più difficile compiere scelte libere.

In questo quadro, le piattaforme assumono così un dominio sempre più grande sulle infrastrutture digitali, definendo regole e condizioni che assumono valenza politica. Ne deriva una perdita di potere da parte dello stato su una risorsa strategica, con una conseguente

[25] S. Sinha, *State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally*, https://iot-analytics.com/number-connected-iot-devices, ultimo accesso gennaio 2026.
[26] Martin, K., & Armstrong, R, *Is the US stock market too concentrated?*, https://www.ft.com/content/2652beb6-c6b8-488e-b189-c1ec926d584b, Ultimo accesso gennaio 2026.

subordinazione alle decisioni di soggetti privati, che operano al di fuori dei tradizionali meccanismi democratici, e una riduzione del controllo sulla proprietà e sull'utilizzo dei dati.

1.4 La dipendenza stato-piattaforme e le scelte tecnologiche

Il potere che deriva alle piattaforme dal controllo, dall'elaborazione e anche dalla produzione di dati riserva loro un potere tale da incidere direttamente anche sulle istituzioni pubbliche, chiamate ad affrontare la necessità di digitalizzazione di sistemi e processi amministrativi, all'interno di un ambiente dominato da pochi provider privati. In questo contesto, il rapporto che si sviluppa tra stato e piattaforme assume una particolare rilevanza, specialmente nel settore del cloud computing.

Numerose istituzioni hanno adottato negli ultimi anni soluzioni cloud esterne come sistemi di calcolo e storage, strumenti per la collaborazione (posta elettronica, videoconferenze, calendari e gestione appuntamenti…) o servizi per la gestione amministrativa, sviluppate da Google, Microsoft o Amazon. Tali soluzioni sono considerate più sicure, flessibili ed efficienti rispetto ai sistemi tradizionali, ma comportano importanti conseguenze in termini di autonomia e controllo dei dati. Questa transizione è stata ulteriormente accelerata dal PNRR, che individua la digitalizzazione come uno degli obiettivi principali.

In questo contesto il rischio di creazione di oligopoli tecnologici, in cui lo stato dipende fortemente da attori privati è molto alto, così come analizzato da Davide Blotta, ricercatore presso la Western Sydney University, riguardo al ruolo di Amazon Web Services nel processo di digitalizzazione dei sistemi di welfare.[27] In assenza di infrastrutture pubbliche le istituzioni sono spinte a esternalizzare la gestione dei dati verso grandi piattaforme, che ricoprono così ruoli essenziali per l'erogazione di servizi. Vengono introdotte in questo modo forme di dipendenza strutturale difficilmente reversibili. Le piattaforme non forniscono più solo un servizio, ma costruiscono l'intero ecosistema informativo sui cui poggiano le politiche pubbliche.

Il cloud non è infatti solo un'infrastruttura, ma incorpora modelli di governance, standard tecnologici e vincoli contrattuali che limitano la capacità dello stato e ne influenzano le scelte. L'uso di cloud esterni comporta fenomeni di lock-in tecnologico, elevati costi di uscita

[27] D. Blotta, *Digitalizzazione dei sistemi di welfare, verso nuovi oligopoli? Il caso di Amazon Web Services*, in Riviste Web, 2023.

e perdita di controllo sui sistemi informativi. Il rischio, di conseguenza, che il potere pubblico perda la proprietà e la funzione di regolatore sulle infrastrutture è elevato, passando ad una posizione di semplice utilizzatore.

Ovviamente, va affermato ancora una volta che le piattaforme non si sostituiscono formalmente allo stato, ma ne condizionano fortemente l'azione. La capacità decisionale non viene abolita, ma progressivamente erosa attraverso la dipendenza da sistemi esterni. Questa dinamica rientra in quanto descritto nel quadro del capitalismo delle piattaforme, queste «si impongono come nuovi attori governamentali veicolando in maniera crescente effetti e processi politici»[28], diventando il luogo in cui definire i rapporti tra stato e capitale.

In questo contesto, la dipendenza stato-piattaforme non riguarda solo la protezione dei dati o la sicurezza informatica, ma anche la capacità di gestione dei processi amministrativi, di programmazione delle politiche pubbliche e la capacità di garantire la continuità dei servizi essenziali. La scelta delle tecnologie diventa così politica, e incide sulla distribuzione del potere e sulle possibilità di controllo democratico.

Al fine di comprendere meglio il tema è stata analizzata la strategia del comune di Parma, che offre un caso studio particolarmente significativo. Rappresenta infatti un tentativo di gestione della dipendenza tecnologica attraverso modelli alternativi ai grandi provider globali. Il percorso di digitalizzazione è basato su un modello ibrido, fondato sull'utilizzo di infrastrutture cloud in house e su una governance tecnica strutturata.

Come emerge da una significativa intervista svolta da chi scrive a Paolo Fontechiari[29], Responsabile della S.O. Infrastrutture Tecnologiche e Telecomunicazioni, la strategia adottata dal comune si articola su due assi principali. Da un lato l'uso dei servizi cloud Lepida, società in house della Regione Emilia-Romagna, dall'altro It.City, società di proprietà interamente del comune, con l'obiettivo di governare l'infrastruttura tecnologica e accelerare il processo di semplificazione e digitalizzazione. Questo assetto ha consentito una razionalizzazione delle infrastrutture ICT, attraverso l'adozione di servizi blade-as-a-service, la centralizzazione dei data center e una gestione più integrata di reti e telecomunicazioni. Tuttavia, nel tempo, tale configurazione, ha assunto progressivamente una forma ibrida, integrando anche

[28] N. Cuppini, M. Frapporti, S. Mezzadra, M. Pirone*, Il capitalismo nel tempo delle piattaforme. Infrastrutture digitali, nuovi spazi e soggettività algoritmiche*, in Rivista Italiana di Filosofia Politica, 2021, p.109.
[29] Intervista realizzata dall'autore in data 29 gennaio 2026 a Paolo Fontechiari, Responsabile della S.O. Infrastrutture Tecnologiche e Telecomunicazioni del Comune di Parma. Trascrizione integrale disponibile in Appendice 1.

cloud esterni certificati. Questa evoluzione è stata determinata sia dagli obblighi introdotti dal PNNR, sia dall'evoluzione del mercato, sempre più orientato verso soluzioni Software-as-a-Service (SaaS). In questo assetto, il fornitore del servizio cloud si occupa anche dello sviluppo, della manutenzione e della distribuzione dei diversi software, rendendoli accessibili agli enti tramite infrastrutture remote e modelli di consumo pay-as-you-go.

Secondo l'intervistato queste scelte hanno ridotto la frammentazione infrastrutturale e migliorato il controllo sui dati. Il modello ha prodotto effetti rilevanti anche in termini di governance, consentendo una maggiore standardizzazione dei processi, un contenimento dei costi e un rafforzamento della sicurezza.

Un «tema centrale non è solo "dove risiedono i dati", ma chi controlla l'infrastruttura, e quali soggetti possono accedere ai dati». Vi è particolare attenzione alla sovranità digitale, e in questa prospettiva la scelta di cloud locali viene definita come una decisione non solo tecnica ed economica, ma anche politica e strategica.

L'obiettivo di ridurre la dipendenza da grandi provider globali viene attuato tramite l'utilizzo di fornitori qualificati secondo l'Agenzia per la Cybersicurezza Nazionale (ACN). Inoltre, grazie a contratti con clausole puntuali, attività di audit continuo e una governance applicativa centralizzata è possibile mantenere un presidio sui flussi informativi.

L'analisi della strategia implementata mostra dunque come un tentativo di riduzione della dipendenza da attori privati sia possibile. Tuttavia, lo stesso responsabile riconosce che questo modello non rappresenta una soluzione definitiva o priva di criticità. Nel lungo periodo i cloud locali possono avere dei limiti in termini di scalabilità, innovazione e difficoltà a competere con hyperscaler globali, che dispongono di risorse nettamente superiori. Inoltre, le normative attualmente esistenti (Regolamento ACN, PSN, NIS2, DORA, Data Act, AI Act) hanno creato una base molto più solida e sicura rispetto al passato, ma nonostante questo non sufficienti per garantire la piena sovranità degli stati. Ad esempio «non forniscono pieno controllo sulla catena tecnologica dell'AI, non risolvono completamente i problemi di portabilità e lock-in, non semplificano gli audit e la supervisione delle infrastrutture esterne».

Il caso evidenzia quindi come la dipendenza stato-piattaforme rimanga una questione aperta. In cui la relazione è strutturalmente asimmetrica, la sovranità decisionale rischia infatti di venire erosa progressivamente dalla tecnologia. Le istituzioni devono adottare per questo motivo misure normative e tecniche, per risolvere un problema che riguarda questioni

tecniche e istituzionali. Il tema della sovranità è quindi centrale nel dibattito contemporaneo, e necessita di un'analisi approfondita dei rischi, delle vulnerabilità e delle risposte normative a livello nazionale ed europeo.

Capitolo 2

Sovranità dei dati e sicurezza

Introduzione

La crescente centralità delle piattaforme rende necessario un approfondimento sul tema del controllo dei dati e delle tecnologie da parte degli stati. I dati sono una risorsa strategica, il cui controllo incide direttamente su equilibri di potere tra mercato e istituzioni. Diventa quindi necessario interrogarsi sulle implicazioni che questa trasformazione produce in termini di autonomia pubblica.

La definizione tradizionale di sovranità, in cui territorio, giurisdizione e infrastrutture coincidevano, è stata messa in crisi dalla digitalizzazione. Questo a causa di un nuovo ecosistema digitale globale, dove la capacità decisionale e operativa di uno stato è sempre più dipendente da infrastrutture gestite da provider privati. In questo contesto emerge il tema della sovranità digitale, intesa come l'effettiva capacità di uno stato di esercitare controllo su dati, tecnologie e infrastrutture alla base della società digitale.

In questo capitolo verrà definito il concetto di sovranità digitale nei documenti strategici dell'Unione Europea, distinguendolo dalla pura sicurezza informatica. Verranno poi analizzate le principali vulnerabilità, derivanti da concentrazione del mercato, dipendenze infrastrutturali e fenomeni di lock-in. Successivamente si procederà con l'esame del quadro normativo europeo e italiano, al fine di valutare se gli strumenti attuali sono in grado di rispondere a tali criticità, grazie anche al supporto di un avvocato esperto in materia di privacy e data protection. Infine, verranno evidenziati i limiti di questo approccio regolatorio, mostrando come la questione della sovranità non sia totalmente gestibile attraverso il mero strumento della legislazione.

2.1 La sovranità digitale nei documenti dell'UE

Nel capitolo precedente abbiamo analizzato come la trasformazione dell'architettura web abbia portato a una centralità delle piattaforme digitali, divenute infrastrutture fondamentali nel mondo contemporaneo, incidendo sia sulle dinamiche economiche che sulla configurazione del potere tra mercato e stato. In questo contesto, investigare il concetto di sovranità

digitale diventa decisamente importante per comprendere deviazioni e tensioni di una formula che di fatto problematizza profondamente la sua dimensione originale. Detta senza mezzi termini, nell'arena digitale oggi pare di scorgere una sfida epocale con profonde implicazioni politiche e concettuali.

Per comprendere la portata di questa sfida, risulta necessario definire cosa intendiamo con il termine sovranità, a partire dalla nozione classica e giuridica del termine. Tradizionalmente, essa è intesa come il potere supremo ed esclusivo di uno stato su un determinato territorio, esercitato attraverso il controllo della forza, la produzione di norme e il controllo delle infrastrutture essenziali[30]. Secondo tale definizione, territorio, giurisdizione e infrastruttura erano tutte circoscritte all'interno di confini definiti, dove era un potere stabilito ad avere la prerogativa: la rete elettrica o di trasporto, ad esempio, essendo collocate fisicamente all'interno dei confini nazionali, restavano soggetti alla piena autorità statale.

Con la digitalizzazione, tuttavia, questa coincidenza viene meno. Le infrastrutture digitali non sono più necessariamente collocate all'interno dei confini nazionali, ma risultano distribuite globalmente. I flussi di dati attraversano giurisdizioni differenti e le diverse tecnologie, come cloud, servizi o algoritmi, sono spesso sviluppate o controllate da multinazionali. Per questo motivo, diviene necessario definire la sovranità in accezione digitale, non più come controllo geografico, ma come la capacità effettiva di uno stato di esercitare pieno controllo sulle infrastrutture digitali, sui dati e sulle tecnologie che garantiscono il funzionamento delle istituzioni, dell'economia e della società. Tale esercizio di controllo si colloca all'interno di una competizione globale tra modelli di governance contrapposti. Da un lato il modello statunitense, di matrice capitalista, caratterizzato dalla centralità di grandi piattaforme private e prevalenza di logiche di mercato. Dall'altro il modello cinese, fondato su una visione centralista e su un controllo statale pervasivo delle infrastrutture e dei flussi informativi. In questo scenario, l'Unione Europea tenta di definire un percorso autonomo, che possa coniugare apertura dei mercati e tutela di diritti e capacità strategica. La sovranità assume dunque una valenza identitaria: la volontà di preservare un modello europeo regolatorio in un contesto globale sempre più frammentato.

Questa esigenza di autonomia e definizione identitaria è stata analizzata dall'European Parliamentary Research Service nel report "Digital sovereignty for Europe", studio di

[30] Treccani, *Sovranità*, in Enciclopedia online, https://www.treccani.it/enciclopedia/sovranita/, ultimo accesso febbraio 2026.

riferimento per fornire un quadro analitico sul significato e sulle implicazioni del concetto di sovranità digitale, in cui si afferma che:

> 'digital sovereignty' refers to Europe's ability to act independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies).[31]

A partire da questa definizione, emerge come la sovranità digitale non possa essere ridotta a una questione tecnica di protezione e cybersicurezza. Nel documento, tale esigenza viene ricondotta alla nozione più ampia di «open strategic autonomy». Con questa espressione l'unione intende rafforzare la capacità di agire autonomamente, in un contesto di interdipendenza globale, evitando però la chiusura del mercato. Quindi la sovranità digitale viene inserita in una strategia politica più ampia, volta a evitare che le scelte infrastrutturali e tecnologiche siano determinate esclusivamente da equilibri industriali esterni. Il tema riguarda la capacità di mantenere margini effettivi di decisione sulla trasformazione tecnologica, andando oltre l'esclusiva protezione dei dati. Queste idee vengono supportate dall'espressione «ability to act independently», che richiama la necessità di un'analisi strategica e politica sul tema, che porti alla definizione di regole comuni del sistema digitale. In altri termini, il punto chiave non è solo la protezione delle infrastrutture, ma soprattutto garantire che le decisioni relative all'architettura digitale non siano subordinate a logiche e interessi privati.

In questa prospettiva, nello stesso report viene affermato che:

> Building a secure pan-European data framework and adopting new standards and practices to provide trustworthy and controllable digital products and services would ensure a safer digital environment, in line with EU values and principles.[32]

Questa affermazione introduce un ulteriore elemento teorico fondamentale, la sovranità implica la necessità di definire standard. Nel contesto tecnologico contemporaneo, il potere legislativo non è esercitabile esclusivamente attraverso norme, ma anche mediante la definizione di protocolli, architetture e modelli. Questi non sono quindi solo strumenti tecnici, ma forme di governo dell'ambiente digitale, chi infatti costruisce standard stabilisce anche le condizioni di funzionamento del sistema.

[31] T. Madiega, *Digital sovereignty for Europe*, European Parliamentary Research Service (EPRS), Briefing Paper, PE 651.992, 2020, p. 1.
[32] Ivi, p. 8.

In questo contesto risulta necessaria una distinzione concettuale tra la sovranità digitale e la sicurezza informatica, le cui definizioni vengono spesso sovrapposte nel dibattito pubblico.

La sicurezza informatica riguarda l'insieme di misure tecniche, organizzative e procedurali volte a «tutelare i sistemi di elaborazione […] dalla possibile violazione, sottrazione o modifica non autorizzata di dati riservati in essi contenuti.»[33]. Essa si concentra su tre dimensioni: la riservatezza, l'integrità e la disponibilità delle informazioni. Al fine di tutelare questi requisiti viene adottato un approccio risk-based, che articola le attività in tre fasi: l'identificazione delle vulnerabilità, la mitigazione dell'impatto di potenziali attacchi e la salvaguardia della continuità operativa dei servizi. In quest'ottica, la sicurezza si integra nell'infrastruttura esistente, operando per consolidarne la resilienza senza alterarne le finalità operative o l'assetto strutturale.

La sovranità digitale, invece, interviene a un livello precedente e più profondo. Come suggerito dal report dell'EPRS, richiama la capacità di esercitare un potere decisionale autonomo rispetto alle condizioni di funzionamento dell'ambiente digitale. Non si tratta soltanto di proteggere un sistema, ma di definire tutte le regole di base: chi controlla l'infrastruttura, chi definisce gli standard, chi stabilisce le modalità di accesso ai dati e chi decide l'evoluzione delle tecnologie.

Questa differenza può essere chiarita distinguendo tra livello operativo e strutturale. La sicurezza opera sul piano operativo, garantendo il funzionamento corretto e protetto di un sistema. Invece, la sovranità opera sul piano strutturale, controllando le infrastrutture e gli standard, incidendo sulla possibilità di modificare l'architettura digitale.

Uno stato può adottare, ad esempio, soluzioni cloud sicure e certificate, tuttavia, se tali soluzioni sono controllate da provider esterni, che impongono condizioni contrattuali sui dati e sull'utilizzo dei sistemi, la capacità pubblica risulta limitata. In questo caso la sicurezza tutela l'integrità del sistema, ma non garantisce un potere decisionale completo sulle condizioni di utilizzo e sulle evoluzioni future.

Un ulteriore elemento riguarda il controllo effettivo sul ciclo di vita del dato. Mentre la sicurezza può essere garantita mediante certificazioni, audit e misure tecniche, la sovranità, invece, implica la capacità di determinare chi può accedere ai dati, a quali condizioni e per

[33] Treccani, *Sicurezza informatica*, in Enciclopedia online, https://www.treccani.it/enciclopedia/sicurezza-informatica/, ultimo accesso febbraio 2026.

quali finalità. L'obiettivo è infatti quello di definire regole di utilizzo e protezione delle informazioni, in un quadro coerente con gli interessi pubblici. Per questi motivi, se le infrastrutture non dipendono direttamente dall'ente pubblico il controllo rimane inevitabilmente incompleto.

In questo senso, la sicurezza informatica costituisce una condizione necessaria ma non sufficiente per garantire la sovranità digitale. Oltre alla protezione dei sistemi è fondamentale assicurarne il governo, affinché lo sviluppo dell'ecosistema digitale possa essere orientato secondo scelte autonome e responsabili.

Occorre allora chiarire in modo preciso quali siano gli elementi che consentono a uno stato di esercitare un'effettiva sovranità digitale. In questa prospettiva il tema dei dati assume una decisiva centralità. Come definiti anche da un documento della Commissione Europea, i dati sono «la linfa vitale dello sviluppo economico»[34]: una risorsa politica e strategica essenziale per il funzionamento di una nazione. Essi sono alla base dei processi decisionali pubblici, della sicurezza nazionale e della competitività di uno stato. La questione principale non è solo proteggere le informazioni, ma avere pieno controllo sull'intero ciclo di vita di un dato, gestendo la creazione, la raccolta, la conservazione, l'elaborazione ma anche la cancellazione e la portabilità.

Proprio in questa direzione si colloca il documento programmatico della commissione europea "Una strategia europea per i dati", in cui viene delineata come deve avvenire la complessiva gestione di questa risorsa. In tale comunicazione si afferma che «l'obiettivo è creare uno spazio unico europeo di dati»[35] in cui essi possano circolare liberamente, nel rispetto di regole comuni e valori condivisi. La strategia li individua come un asset per la crescita economica, la competitività e il progresso della società, sottolineando che la gestione autonoma di questi è una condizione essenziale per l'Europa.

In questo quadro, la sovranità viene declinata come sovranità sui dati. Essa implica la capacità di decidere dove i dati sono conservati, chi può accedervi e a quali condizioni. Riguarda la protezione di tutti i dati, siano essi personali, pubblici o riguardanti aziende. Non si tratta di una concezione territoriale della sovranità, bensì una forma di controllo funzionale e

[34] Commissione Europea, *Una strategia europea per i dati*, in Comunicazioni della Commissione Europea, COM (2020) 66, 2020, p. 4.
[35] Ivi, p. 6.

normativo. Infatti, la localizzazione fisica dei server non garantisce la piena sovranità digitale se i dati e le infrastrutture sono controllati da attori esterni.

In secondo luogo, la strategia europea evidenzia come la sovranità non debba essere implementata attraverso l'autarchia o l'isolazionismo, ma attraverso la capacità di agire in modo autonomo all'interno del mercato. Come viene sottolineato nella comunicazione, l'obiettivo è rafforzare la "strategic autonomy" dell'Unione, garantendo che non vengano imposte scelte tecnologiche da attori esterni o determinate esclusivamente da dinamiche di mercato.

Sotto un profilo più tecnico, è necessario agire su più livelli dello spazio digitale. Un elemento di fondamentale importanza è la connettività, su cui si basano tutti i servizi; infatti, senza la gestione delle infrastrutture di rete ogni discorso sulla sovranità risulterebbe incompleto. Su questa base è fondata la capacità di calcolo e di archiviazione, formata dalla disponibilità di data center, cloud infrastrutturali e servizi computing, «in tale ottica è necessario che l'UE riduca le proprie dipendenze tecnologiche»[36], scrive ancora il Report. Questo apparato richiede poi una cybersicurezza pervasiva; infatti, la protezione delle infrastrutture critiche e dei dati sensibili è indispensabile per garantire continuità operativa. Infine, risulta necessaria una chiara strategia di governance dei dati, ossia la capacità di definire regole comuni per garantire l'interoperabilità, la portabilità e la condivisione, evitando così frammentazioni o dipendenze strutturali.

Proprio da questo profilo tecnico appena descritto emerge il legame tra sovranità e standardizzazione. La capacità di definire standard tecnici, protocolli e criteri di certificazione rappresenta infatti un elemento centrale della sovranità digitale. Gli standard sono strumenti normativi, non solo tecnici, che stabiliscono le condizioni di accesso al mercato e il funzionamento dell'ecosistema digitale. In assenza di questi, uno stato rischia di dover adottare soluzioni sviluppate da altri soggetti, accettandone logiche, priorità e modelli di governance.

In questa ottica, l'Unione Europea la considera una condizione necessaria per garantire sicurezza e autonomia strategica, affermando che:

> se vuole conquistarsi un ruolo guida nell'economia dei dati, l'UE deve agire subito e affrontare in maniera concertata questioni che vanno dalla connettività all'elaborazione e alla conservazione dei dati, dalla potenza di calcolo alla cibersicurezza.[37]

[36] Ivi, p. 2.
[37] Ivi, p. 11.

Inoltre, è possibile comprendere la necessità di controllo dell'intera infrastruttura dell'economia dei dati. Non è sufficiente controllare il solo livello applicativo se le infrastrutture sottostanti, come hardware, cloud o sistemi operativi, restano nelle mani di pochi soggetti privati. La sovranità, pertanto, deve essere intesa come una condizione che attraversa l'intero stack tecnologico, dalla produzione dei dati, alla loro elaborazione e conservazione.

Infine, la sovranità digitale presenta anche una dimensione istituzionale. Senza una pubblica amministrazione in grado di supervisionare le infrastrutture digitali, anche soluzioni tecnicamente sicure non assicurano un reale controllo. La sovranità digitale si configura quindi come un concetto multidimensionale, che integra capacità strategica, standardizzazione tecnica e autonomia decisionale.

Questa impostazione ha progressivamente orientato l'Unione verso strumenti che permettessero di rafforzare anche la dimensione infrastrutturale della sovranità. Accanto alle norme, si è infatti affermata l'esigenza di incidere direttamente sulle capacità tecnologiche europee, sviluppando progetti come GAIA-X di cui parleremo in più avanti.

La riflessione europea sulla sovranità digitale si sviluppa, inoltre, come una risposta alla vulnerabilità globale dell'ecosistema tecnologico. Nei documenti viene più volte sottolineato come la concentrazione della capacità di calcolo, delle infrastrutture cloud, delle piattaforme, e delle tecnologie emergenti.

2.2 Vulnerabilità, problemi e rischi per lo stato

Dopo aver definito la sovranità digitale come la capacità di controllo da parte di uno stato sulle infrastrutture e sui dati, occorre ora comprendere quali vulnerabilità emergono quando tale controllo risulta indebolito o parziale. La questione non è puramente teorica, ma si manifesta concretamente quando le pubbliche istituzioni sono chiamate a organizzare i servizi pubblici, gestire le infrastrutture digitali o trattare i dati all'interno di sistemi spesso governati da soggetti privati globali.

Uno dei principali problemi riguarda la concentrazione del mercato delle infrastrutture digitali, in particolare nel settore del cloud computing. Lo studio del parlamento europeo "European Software and Cyber Dependencies"[38] evidenzia come il mercato del cloud sia

[38] V. Gineikyte-Kanclere et al., *European Software and Cyber Dependencies*, European Parliament, PE 780.413, 2025, p. 1.

caratterizzato da una significativa concentrazione e da una posizione dominante di provider extraeuropei, in particolare AWS, Microsoft e Google detengono complessivamente circa il 70% della quota di mercato, mentre SAP, il più grande fornitore cloud europeo, si attesta solamente attorno al 2%. Tale configurazione genera una dipendenza strutturale di natura sia economica che strategica. Infatti, quando un'amministrazione pubblica migra verso un'infrastruttura cloud, affida a soggetti esterni componenti essenziali della propria capacità operativa.

In questo contesto emerge il problema del vendor lock-in, inteso come l'insieme di difficoltà tecniche, economiche e organizzative di migrare verso un altro provider una volta adottata una soluzione digitale. Tale dipendenza non è causata strettamente da vincoli contrattuali o clausole restrittive, ma anche da scelte architetturali del sistema, come l'adozione di standard proprietari, lo sviluppo di configurazioni personalizzate, o l'uso di licenze. In tali condizioni, la migrazione verso soluzioni alternative comporta switching costs elevati, in termini di costi, rischi e dispersione del know-how. Quindi la libertà formale di cambiare fornitore tende a trasformarsi in una dipendenza sostanziale.

Un caso emblematico è rappresentato dal Comune di Göteborg, oggetto di uno studio condotto da un gruppo di professori e ricercatori di computer science all'Università di Skövde in Svezia[39]. La ricerca analizza le criticità emerse dopo l'adozione di Microsoft 365 come soluzione per la gestione documentale. I documenti infatti venivano archiviati nel formato OOXML (ISO/IEC 29500), formalmente uno standard ISO internazionale interoperabile, ma sviluppato da Microsoft. Quindi la sua implementazione concreta risultava fortemente integrata nell'ecosistema del fornitore e poteva includere estensioni, funzionalità o riferimenti a standard coperti da brevetti, la cui gestione richiedeva specifiche licenze. Inoltre, il comune non aveva verificato e acquisito tutti i diritti per garantire la manutenzione autonoma dei propri documenti, indipendentemente dalla piattaforma. Di conseguenza, pur potendo esportare e accedere ai file con altri software, la piena interoperabilità, la corretta conservazione e la possibilità di migrare verso un'altra soluzione avrebbe comportato problemi e costi significativi. Il lock-in si è configurato quindi come una dipendenza ecosistemica derivata da

[39] Björn Lundell et al., *Avoiding lock-in effects through obtaining all necessary licences before use of a SaaS solution in a public sector organisation: a case study*, in European Journal of Law and Technology, vol. 14, n. 1, 2023.

standard formalmente aperti, implementazioni proprietarie e carenze nell'analisi delle licenze e delle condizioni contrattuali.

Tuttavia, la dipendenza non riguarda solo le piattaforme proprietarie. Come evidenziato dallo studio di Per Persson, ricercatore presso l'University of Gothenburg e Johan Linåker[40], ricercatore presso il RISE Research Institutes of Sweden, possono esistere dei soft-lock-in legati all'utilizzo di software open-source. Nell'articolo, i ricercatori analizzano il caso relativo ad una piattaforma ESP, adottata da oltre 190 comuni in Svezia per la gestione dei servizi amministrativi. Sebbene il codice fosse accessibile e modificabile, si sono comunque generate forme di dipendenza: le amministrazioni avevano accumulato personalizzazioni e integrazioni difficilmente trasferibili e l'eventuale riconfigurazione del sistema avrebbe richiesto investimenti elevati. Inoltre, tra gli sviluppatori e gli enti pubblici si erano create delle asimmetrie informative, rafforzando ancora di più la dipendenza. Questo caso ha dimostrato che l'apertura del software non ha automaticamente impedito la formazione di lock-in, a causa della configurazione complessiva della piattaforma.

Accanto alla dipendenza economica e contrattuale analizzata, le vulnerabilità create dalla perdita di sovranità digitale assumono una portata più ampia, includendo questioni giuridiche, tecniche e politiche tra loro connesse. Il tema non riguarda solamente un aumento dei costi o una diminuzione dell'efficienza, ma investe la capacità di uno stato di esercitare un controllo effettivo sull'ambiente digitale in cui opera.

In primo luogo, emerge una vulnerabilità sul piano giuridico e geopolitico. Quando i dati sono trattati da provider extraeuropei possono essere soggetti a normative straniere che prevedono forme di accesso da paesi terzi. Su questo tema il caso del Cloud Act statunitense è emblematico, esso permette alle autorità americane di richiedere ai cloud provider l'accesso ai dati detenuti da società americane, indipendentemente dal luogo in cui questi sono conservati. In simili circostanze, la sovranità si frammenta e viene generato un possibile conflitto tra gli ordinamenti, nel quale uno stato europeo può trovare limitazioni nella capacità di impedire accessi o trasferimenti non desiderati. Questa tensione riflette la dimensione globale delle infrastrutture e può portare a rischi concreti per la sicurezza nazionale.

[40] P. Persson, J. Linåker, *Soft-lockins in Public Sector Acquisitions of Open Source Software-solutions: A Case Study on a Municipal E-Service Platform*, Cornell University, arXiv preprint, 2024.

A questa dimensione giuridica si affianca una vulnerabilità tecnica. L'ENISA, ovvero l'Agenzia dell'Unione Europea per la Cibersicurezza, nel rapporto ETL 2025 sul panorama delle minacce, sottolinea come la crescente digitalizzazione delle infrastrutture abbia ampliato la superficie di attacco. Questo è causato dall'architettura particolarmente complessa dei cloud, caratterizzata da virtualizzazione avanzata, distribuzione geografica dei data center e interconnessione tra i sistemi, elementi che rendono la gestione del rischio più complessa rispetto ai modelli tradizionali in-house. In particolare, il rapporto afferma che l'«abuse of cyber dependencies»[41] sta intensificando il rischio «throughout interconnected digital ecosystems». In questo scenario, un incidente può produrre effetti a catena, incidendo simultaneamente su più istituzioni o servizi essenziali.

Tale dinamica è alimentata dalla crescente concentrazione delle infrastrutture digitali, la quale genera una forma di rischio legato alla supply chain tecnologica. Nel momento in cui numerose amministrazioni dipendono da unici fornitori, un singolo punto di compromissione può propagarsi lungo l'intera catena del valore digitale. In quest'ottica la dipendenza emerge come un fattore strutturale, che amplifica l'impatto delle minacce e riduce la capacità di intervento in caso di incidenti. La vulnerabilità, dunque, deriva dall'architettura stessa dell'ecosistema digitale interconnesso.

Tuttavia, la vulnerabilità non si esaurisce nella dimensione tecnica, ma assume anche una dimensione strategica. Nel momento in cui un'amministrazione integra i propri servizi in un ecosistema gestito esternamente, accetta che l'evoluzione del sistema sia determinata principalmente da logiche industriali e commerciali del fornitore. Si determina così un condizionamento indiretto delle politiche pubbliche, che vincola lo stato a standard, architetture e roadmap tecnologiche di attori privati, limitando l'autonomia di innovazione nazionale.

Questa dipendenza non riguarda solo la possibilità di migrazione verso un altro provider, ma la progressiva perdita di controllo sullo sviluppo tecnologico. Se i provider decidono di modificare o aggiornare le infrastrutture su cui poggiano i servizi pubblici essenziali, secondo le loro priorità, le amministrazioni sono obbligate a adattarsi a scelte che non hanno contribuito a definire. Tale dipendenza produce una forma di lock-in strategico, in cui la dipendenza non è immediatamente visibile sul piano contrattuale, ma si manifesta attraverso l'evoluzione dell'ecosistema tecnologico.

[41] ENISA - European Union Agency for Cybersecurity, *ENISA Threat Landscape 2025*, ENISA, 2025, p. 7.

Accanto a questa dimensione strategica si colloca una vulnerabilità istituzionale. Spesso le amministrazioni non sono in grado di comprendere pienamente l'architettura dei sistemi adottati, a causa della complessità di tali soluzioni, che richiederebbero competenze tecniche avanzate per capirne il funzionamento. In assenza di tali competenze, si genera un'asimmetria informativa tra amministrazione e fornitore. Il provider conosce a pieno l'infrastruttura, mentre l'ente pubblico utilizza i servizi senza possederne il controllo completo. Questa asimmetria può limitare la capacità negoziale delle istituzioni, limitando anche la possibilità di valutare rischi e alternative autonomamente.

Riprendendo l'intervista fatta a Paolo Fontechiari, Responsabile della S.O. Infrastrutture Tecnologiche e Telecomunicazioni del Comune di Parma[42], emerge che il problema non è soltanto "dove risiedono i dati", ma chi governa l'infrastruttura ed entro quali margini l'ente pubblico può intervenire. Infatti, la scelta del comune di utilizzare soluzioni in-house è stata dettata dalla volontà precisa di mantenere competenze interne e mantenere un controllo sull'evoluzione dei sistemi. Ciò dimostra che le vulnerabilità devono essere percepite come rischio di possibile erosione delle capacità decisionali degli enti.

Un'ulteriore vulnerabilità riguarda la natura dei dati trattati. Questi dati detenuti dalle amministrazioni sono molto spesso sensibili, riguardanti temi di sicurezza nazionale, informazioni private degli individui o sulla pianificazione strategica dello stato. Quando la loro gestione viene affidata a privati, possono nascere dubbi sulla riservatezza, sulla protezione o sull'accesso da parte di terzi, dato che l'infrastruttura non è pienamente sotto il controllo dello stato. Non a caso, il Data Governance Act, pilastro normativo riguardante la strategia europea dei dati, richiama la necessità di tutelare gli interessi pubblici, riconoscendo che il trasferimento dei dati può entrare in conflitto con questo obiettivo.

Infine, è rilevante menzionare una vulnerabilità propriamente politica. Il controllo dei dati implica l'esercizio di forme di potere sugli individui, incidendo su comportamenti individuali e collettivi. Se questo viene applicato al contesto pubblico, il rischio che decisioni statali siano influenzate da logiche algoritmiche non controllate democraticamente è molto alto. La perdita di sovranità digitale si traduce quindi in una fragilità che investe l'intera azione statale, poiché il governo dei dati diventa, in ultima analisi, una questione di potere.

[42]Intervista realizzata dall'autore in data 29 gennaio 2026 a Paolo Fontechiari, Responsabile della S.O. Infrastrutture Tecnologiche e Telecomunicazioni del Comune di Parma. Trascrizione integrale disponibile in Appendice 1.

Nel loro insieme, queste vulnerabilità dimostrano come una minore sovranità porti a una trasformazione strutturale del rapporto tra stato e infrastrutture. Quando il controllo dell'ecosistema digitale è frammentato, anche la capacità decisionale risulta condizionata. È proprio su questi temi che verrà svolta una valutazione del quadro normativo europeo, per comprendere se gli strumenti giuridici vigenti siano idonei ad assicurare autonomia e controllo.

2.3 Il quadro normativo italiano ed europeo

Le vulnerabilità e i problemi analizzati nel paragrafo precedente hanno portato l'Unione Europea e in parte lo Stato italiano, a sviluppare un quadro normativo volto a governare la trasformazione digitale. Il punto ora è quindi analizzare questi strumenti e comprendere se e in quale misura, sono in grado di incidere sulla sovranità digitale, o se si limitano a intervenire solo sul piano della sicurezza e gestione del rischio.

Il fondamento politico di tale percorso è da ritrovare nella Strategia Europea per i Dati[43], attraverso la quale l'Europa ha progressivamente costruito una vera e propria architettura regolatoria. In tale documento programmatico, i dati vengono individuati come risorsa strategica per la crescita economica, l'innovazione, il funzionamento delle pubbliche amministrazioni e la competitività complessiva dell'Unione. L'obiettivo è costruire uno spazio unico europeo dei dati, favorendo la circolazione e il riutilizzo delle informazioni all'interno dell'UE. Parallelamente, la strategia evidenzia l'importanza di dotarsi di adeguati strumenti per garantire un utilizzo dei dati conforme ai requisiti di sicurezza e protezione.

Tuttavia, la strategia non si esaurisce in una prospettiva di mercato, ma si inserisce in un progetto più ampio per garantire l'autonomia strategica europea. Per questo si individua nella governance dei dati una condizione essenziale per ridurre le dipendenze strutturali da attori terzi, disciplinando l'accesso, l'utilizzo e la condivisione delle informazioni secondo interessi europei.

Su tale base è possibile elencare una serie di atti normativi vincolanti in materia di dati, sia europei che italiani. Tra cui figurano il GDPR, il Data Governance Act, il Data Act, la Direttiva NIS2, lo schema EUCS e le iniziative italiane ACN e PSN. A confermare questo quadro

[43] Commissione Europea, *Una strategia europea per i dati*, in Comunicazioni della Commissione Europea, COM (2020) 66, 2020.

è l'Avvocato Francesco Montesi, consulente legale in privacy e data protection, come emerge da una significativa intervista svolta da chi scrive[44] per analizzare il tema.

Il primo riferimento è il GDPR, ovvero il Regolamento (UE) 2016/679. Pur non essendo stato concepito esplicitamente come strumento di sovranità digitale, e pubblicato anni prima della Strategia europea per i dati, ha avuto un grande impatto sulla capacità dell'Unione di esercitare un potere regolatorio. Infatti, viene stabilito il principio di extraterritorialità nell'articolo 3, dove si afferma che il regolamento si applica a tutti i soggetti responsabili del trattamento dei dati, «indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione»[45]. Inoltre, gli articoli 44-49 disciplinano il trasferimento di dati verso paesi terzi, subordinandoli alla presenza di adeguate garanzie. In particolare, un passaggio dell'articolo 44 stabilisce che il trasferimento può avere luogo «soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento.»[46]

Sotto questo profilo, il GDPR rafforza la capacità regolatoria europea. Infatti, come evidenziato nell'intervista citata, può essere considerato rilevante anche in ottica di sovranità dei dati, poiché consente di mantenere un controllo effettivo sul trattamento dei dati e sui loro trasferimenti verso paesi terzi. In particolare, la disciplina del capo V e il principio di extraterritorialità attribuiscono al diritto europeo una portata che supera i confini dell'Unione, rafforzando la capacità di incidere anche su operatori globali. Resta tuttavia centrale la sua finalità originaria di tutela dei diritti fondamentali degli interessati, e la protezione dei dati personali. Il suo contributo, quindi, pur significativo, non incide pienamente sul problema del controllo infrastrutturale e riduzione delle dipendenze.

Un passo ulteriore viene compiuto con il Data Governance Act (DGA), ovvero il Regolamento (UE) 2022/868. Tale atto mira a creare meccanismi sicuri per la condivisione dei dati, con particolare attenzione a quelli detenuti da enti pubblici. Vengono introdotti strumenti per garantire tutele di sicurezza pubblica, quali servizi di intermediazione dei dati negli articoli 10-14, e modalità di riutilizzo di certe categorie di dati pubblici protetti negli articoli 3-9, in

[44] Intervista realizzata dall'autore in data 22 febbraio 2026 a Francesco Montesi, consulente legale in privacy e data protection. Trascrizione integrale disponibile in Appendice 2.
[45] Parlamento Europeo, Consiglio dell'Unione Europea, *Regolamento (UE) 2016/679 (GDPR)*, in Gazzetta ufficiale dell'Unione Europea, L 119,2016, p. 32.
[46] Ivi, p.60.

particolare da «riservatezza commerciale, riservatezza statistica, protezione dei diritti di proprietà intellettuale di terzi o protezione dei dati personali»[47].

Sebbene il DGA riconosca i rischi che il trasferimento e la condivisione dei dati possono portare, anche in questo caso, la regolazione si basa sulla governance e sull'accesso, più che sull'infrastruttura sottostante. Il regolamento, quindi, non interviene direttamente sulla dipendenza dai provider, nonostante crei maggiore fiducia nella condivisione dei dati.

Più esplicita è la disciplina introdotta dal Data Act, ovvero il Regolamento (UE) 2023/2854, almeno sul piano delle dipendenze e del lock-in. Questo regolamento affronta il tema della portabilità e dell'accesso ai dati, generati in un ecosistema di servizi. Specialmente gli articoli 23-31 sono particolarmente rilevanti ai fini della sovranità digitale, perché presentano disposizioni relative alla mobilità tra fornitori di servizi di elaborazione dati, riducendo ostacoli tecnici e contrattuali alla migrazione tra diversi cloud.

In particolare, l'articolo 23 stabilisce che i provider «non impongono ed eliminano in particolare gli ostacoli pre-commerciali, commerciali, tecnici, contrattuali e organizzativi»[48], definendo così obblighi ai fornitori di rimozione delle barriere alla portabilità, vietando clausole contrattuali che ostacolino il passaggio a un altro fornitore. Inoltre, il regolamento promuove interoperabilità e standardizzazione tecnica, proprio al fine di mitigare fenomeni di lock-in.

Il Data Act rappresenta quindi un tentativo di incidere sulle dinamiche di dipendenza, però si colloca ancora in una logica di regolazione del mercato e promozione della concorrenza, non imponendo scelte infrastrutturali o limitando la concentrazione del settore.

Parallelamente alla disciplina dei dati, l'Unione Europea ha innalzato i livelli di cibersicurezza attraverso la Direttiva (UE) 2022/2555 (NIS2), che introduce un nuovo quadro normativo per la sicurezza di reti e sistemi. La direttiva impone requisiti più stringenti in materia di gestione del rischio, includendo un numero maggiore di settori strategici e soggetti a cui vengono applicati gli obblighi. Inoltre, le nuove norme introducono l'obbligo di notifica tempestiva degli incidenti e sanzioni più incisive. In particolare, l'articolo 21 stabilisce che

[47] Parlamento Europeo, Consiglio dell'Unione Europea, *Regolamento (UE) 2022/868 (Data Governance Act),* in Gazzetta ufficiale dell'Unione Europea, L 152, 2022, p. 21.
[48] Parlamento Europeo, Consiglio dell'Unione Europea, *Regolamento (UE) 2023/2854 (Data Act),* in Gazzetta ufficiale dell'Unione Europea, L 2023/2854, 2023, p. 54.

> Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi.[49]

Sebbene la NIS2 rafforzi la resilienza e la protezione delle infrastrutture critiche, si concentra per lo più nell'ambito della cybersecurity. In altri termini, la sicurezza viene rafforzata, riducendo l'esposizione agli attacchi e cercando di garantire la continuità operativa, ma non viene necessariamente consolidata la sovranità, non si interviene, infatti, sulla concentrazione del potere o sulle infrastrutture.

Oltre a ciò, il legislatore italiano ha istituito l'Agenzia per la Cybersicurezza Nazionale (ACN), ovvero l'autorità che ha il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico. Essa si occupa di prevenire e mitigare gli attacchi e di favorire il raggiungimento dell'autonomia tecnologica.

In questo quadro si colloca il progetto del Polo Strategico Nazionale (PSN), una delle principali iniziative per la costruzione di un'infrastruttura digitale nazionale in grado di concretizzare il principio di autonomia tecnologica e sovranità dei dati. Esso rappresenta il tentativo italiano di intervenire direttamente sull'infrastruttura, distaccandosi in parte dal metodo europeo basato principalmente sulla regolazione. L'obiettivo del PSN è dotare la pubblica amministrazione italiana di un infrastruttura cloud avanzata, sicura, efficiente e resiliente, capace di ospitare dati e servizi con standard elevati di protezione e indipendenza tecnologica.[50] Il progetto nasce nell'ambito della "Strategia Cloud Italia" promossa dal Dipartimento per la Trasformazione Digitale, con un modello di governance pubblico-privato che coinvolge i principali attori nazionali dell'industria ICT come TIM e Leonardo.

L'architettura tecnica del PSN è stata concepita per garantire la gestione e protezione di dati critici e strategici delle amministrazioni pubbliche. L'infrastruttura fisica di questo sistema è basata su un insieme di data center distribuiti sul territorio nazionale, il cui obiettivo è

[49] Parlamento Europeo, Consiglio dell'Unione Europea, *Direttiva (UE) 2022/2555 (NIS2)*, in Gazzetta ufficiale dell'Unione Europea, L 333, 2022, p. 48.
[50] Polo Strategico Nazionale, *Chi siamo*, https://www.polostrategiconazionale.it/chi-siamo/polo-strategico-nazionale/, ultimo accesso febbraio 2026.

garantire resilienza e continuità operativa, consentendo la replicazione dei servizi e tolleranza ai guasti anche in caso di interruzioni locali.[51]

Dal punto di vista dell'offerta tecnologica, il PSN adotta un modello di cloud eterogeneo, che combina infrastrutture proprietarie e servizi di provider esterni qualificati. Grazie a tale approccio, le pubbliche amministrazioni possono accedere a servizi di hosting, storage e protezione dei dati, oltre ai modelli IaaS e PaaS.[52] Nello specifico, con i servizi *IaaS* intendiamo un modello di cloud computing in cui il provider fornisce risorse infrastrutturali virtualizzate (come server o storage) in modalità on demand: l'utilizzatore mantiene il controllo su sistemi operativi e applicazioni, mentre è compito del fornitore gestire e mantenere l'infrastruttura. Con il modello *PaaS,* invece, il provider eroga una piattaforma completa, che include infrastruttura, sistema operativo e ambiente di sviluppo, consentendo all'utilizzatore di concentrarsi sulla creazione e sull'esecuzione del software.

Un esempio di come viene composta questa infrastruttura è il servizio Public Cloud PSN Managed[53], che consente alle istituzioni di usare soluzioni cloud integrate e gestite all'interno dell'infrastruttura. Questo servizio si basa su tecnologie come Google Assured Workload, soluzione di Google progettata per creare ambienti cloud che rispettano specifici requisiti normativi e di sicurezza. Tali ambienti prevedono vincoli sulla localizzazione dei dati e sul loro accesso, e per questo sono ospitati in data center collocati sul territorio italiano.

La gestione di questi servizi segue criteri di controllo e supervisione, in cui personale specializzato si occupa del mantenimento tecnologico e dell'integrazione dei processi di sicurezza e conformità. Grazie a matrici di responsabilità condivisa i ruoli tra fornitore del servizio e amministrazione pubblica vengono delineati, rafforzando il controllo dello stato e permettendo la tracciabilità e la difesa di dati e sistemi.

Per quanto riguarda invece la sovranità digitale, il valore aggiunto del PSN risiede nella capacità di controllo dell'intero ciclo di vita di dati e servizi, andando oltre la sola protezione tecnica dei sistemi. Infatti, la dipendenza da cloud esterni viene ridotta controllando la locazione fisica e disciplinando l'accesso attraverso infrastrutture soggette a governance

[51] Dipartimento per la trasformazione digitale, *Strategia Cloud Italia - La strategia cloud per la Pubblica Amministrazione*, in Docs Italia, https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/stabile/4_la_strategia_cloud_per_la_pubblica_amministrazione.html, ultimo accesso febbraio 2026.
[52] Polo Strategico Nazionale, *Soluzioni*, https://www.polostrategiconazionale.it/soluzioni/, ultimo accesso febbraio 2026.
[53] Polo Strategico Nazionale, *Public Cloud*, https://www.polostrategiconazionale.it/soluzioni/servizi-con-cloud-service-provider/public-cloud/, ultimo accesso febbraio 2026.

pubblica. Inoltre, viene rafforzato il controllo sui processi di elaborazione, conservazione e fruizione delle informazioni.

L'infrastruttura è inoltre progettata per accompagnare le amministrazioni alla migrazione al cloud, affidandosi a un ambiente standardizzato e qualificato, riducendo la complessità gestionale e garantendo livelli di conformità normativa e sicurezza. In questa prospettiva, rappresenta uno strumento di coordinamento e rafforzamento del controllo pubblico dell'ecosistema digitale.

Secondo quanto emerso dall'intervista con l'Avv. Montesi, il regolamento ACN e il PSN rappresentano un passaggio significativo anche sul piano infrastrutturale, poiché introducono obblighi per i fornitori e criteri stringenti di localizzazione e verifica dei dati, che incidono sulle scelte delle soluzioni cloud da parte delle amministrazioni. Dal punto di vista strettamente giuridico, tali strumenti possono quindi essere letti come forme di rafforzamento della sovranità digitale, in quanto limitano la discrezionalità nella selezione dei provider e impongono requisiti di sicurezza e affidabilità.

Infine, un ulteriore elemento di rilievo è lo sviluppo dello schema europeo di certificazione della cybersicurezza per i servizi cloud (EUCS), nell'ambito del Regolamento (UE) 2019/881, ovvero Cybersecurity Act[54]. Questo schema di certificazione punta a introdurre una serie di requisiti relativi alla valutazione dei servizi, alla gestione dei rischi, alla continuità dei dati e alla loro protezione. Introduce inoltre diversi livelli di affidabilità, fondamentali per valutare i cloud in base al livello di sicurezza garantito, permettendo il rafforzamento della capacità decisionale degli enti pubblici. Anche qui, l'intervento si concentra sulla compliance tecnica e sui requisiti di sicurezza, senza necessariamente incidere sulla proprietà o sul controllo strategico delle infrastrutture.

Nel complesso, dal punto di vista giuridico, il quadro normativo europeo e nazionale appare solido, la sovranità digitale trova una base consistente. Le norme analizzate non si limitano alla gestione del rischio, ma intervengono sul governo dei dati, sulla portabilità e su molti altri temi.

Tuttavia, la questione va analizzata su un piano ulteriore. Se la sovranità viene intesa non soltanto come capacità regolatoria, ma come pieno controllo e autonomia nella gestione delle

[54] Parlamento Europeo, Consiglio dell'Unione Europea, *Regolamento (UE) 2019/881 (Cybersecurity Act*), in Gazzetta ufficiale dell'Unione Europea, L 151, 2019.

infrastrutture e dei servizi digitali, occorre interrogarsi sulla sufficienza di un approccio fondato prevalentemente sulla regolazione. La risposta a tale interrogativo richiede un'analisi che vada oltre il piano strettamente giuridico e consideri la dimensione strutturale e operativa dell'ecosistema digitale europeo.

2.4 I limiti dell'approccio normativo alla sovranità digitale

Dall'analisi del quadro normativo europeo svolta nel precedente paragrafo – certo solo approcciata, ma nondimeno ripresa nelle sue parti essenziali –, abbiamo compreso come l'Unione abbia costruito un sistema regolatorio complesso per garantire la sicurezza digitale, disciplinare l'uso dei dati e favorirne la circolazione. Tuttavia, sono emerse delle criticità su cui è necessario interrogarsi per comprendere i limiti di questo approccio. La questione centrale non riguarda l'efficacia delle singole norme, ma la loro capacità di proteggere le istituzioni da dinamiche di concentrazione e dipendenza che caratterizzano l'ecosistema digitale.

In primo luogo, emerge un limite di tipo strutturale, dato che le normative europee non intervengono sulla proprietà o sul controllo delle infrastrutture, ma prevalentemente sulla regolazione dell'uso e la gestione del rischio. Dall'analisi possiamo comprendere che il GDPR disciplina il trattamento dei dati personali, ma non è stato concepito come strumento per incidere sulla struttura del mercato dei cloud. In modo analogo, il Data Governance Act e il Data Act non modificano in modo diretto la concentrazione degli operatori hyperscale, ma intervengono sulle condizioni di accesso, condivisione e portabilità dei dati, cercando di ridurre le difficoltà nel cambio di provider. La NIS2, infine, rafforza resilienza e sicurezza di reti e sistemi, ma non affronta direttamente la questione di dipendenza tecnologica o controllo infrastrutturale, rimanendo principalmente nel perimetro della cybersecurity.

Questa impostazione è stata oggetto di riflessione anche nello studio dell'EPRS "Digital sovereignty for Europe"[55], che ha evidenziato come l'"open strategic autonomy" europea si fonda su un equilibrio tra apertura dei mercati e riduzione delle dipendenze, ma da solo questa strategia non è sufficiente a colmare i divari tecnologici consolidati. Analogamente nel documento "2030 Digital Compass", la Commissione Europea ha sottolineato come la sovranità non possa essere garantita esclusivamente dalle normative, ma necessita di investimenti strutturali e innovazione tecnologica interna, affermando che l'UE deve «strengthen

[55] T. Madiega, *Digital sovereignty for Europe*, European Parliamentary Research Service (EPRS), Briefing Paper, PE 651.992, 2020.

its own cloud infrastructure and capacities»[56] al fine di colmare il gap nella capacità di elaborazione dati.

Un secondo limite di questo approccio riguarda la difficoltà di portabilità e il conseguente lock-in. Sebbene il Data Act introduca obblighi per facilitare il passaggio tra fornitori diversi, la complessità delle migrazioni, l'integrazione tra piattaforma e infrastruttura e il livello di personalizzazione dei sistemi, come già visto in alcuni esempi del secondo paragrafo, continuano a rappresentare degli ostacoli concreti. In un'analisi dedicata al tema, Gianluca Marcellino, Demand Manager presso l'Area Innovazione Tecnologica e Digitale del Comune di Milano, individua tre cause principali che portano al lock in: l'uso di tecnologie esclusive, condizioni contrattuali rigide e la carenza di competenze necessarie per il trasferimento di dati e servizi.[57]

Nello stesso contributo viene collegato il problema alla dimensione della sovranità. Infatti, la crescente dipendenza da fornitori extraeuropei accentua le asimmetrie di potere contrattuale e rende più fragile la continuità operativa in caso di decisioni unilaterali dei provider. Inoltre, l'articolo richiama come l'origine di queste difficoltà sia legata anche a modelli contrattuali rigidi a favore dei fornitori, come osservato da Gabriele Faggioli, CEO di Partners4Innovation e presidente onorario del CLUSIT (Associazione Italiana per la Sicurezza Informatica), evidenziando come le barriere non siano solo tecniche, ma spesso incorporate nelle condizioni economiche e giuridiche dei servizi cloud.

Questa lettura trova riscontro anche a livello operativo nelle amministrazioni pubbliche, come affermato da Paolo Fontechiari nell'intervista già citata, il quale evidenzia come «le normative attuali […] non risolvono completamente i problemi di portabilità e lock-in», poiché le barriere tecniche e organizzative non vengono eliminate automaticamente dagli obblighi normativi, ma è necessario applicare anche modifiche strutturali. In questo senso, l'esperienza concreta delle amministrazioni conferma un limite strutturale all'approccio regolatorio.

Un ulteriore limite può essere individuato nella dimensione amministrativa e operativa. Sono necessarie, infatti, elevate competenze e risorse per adempiere a tutti gli obblighi delle

[56] Commissione Europea, *2030 Digital Compass: the European way for the Digital Decade*, COM (2021) 118 final, 2021, p. 8.
[57] Gianluca Marcellino*, Lock in del cloud, come tutelarsi: i consigli dei fornitori del servizio*, in Agenda Digitale, https://www.agendadigitale.eu/infrastrutture/lock-in-del-cloud-come-tutelarsi-i-consigli-dei-fornitori-del-servizio, ultimo accesso febbraio 2026.

normative, che possono talvolta sovrapporsi tra loro. In assenza di tali risorse il rischio è che la regolazione si traduca in un aumento degli oneri burocratici, senza rafforzare in modo sostanziale la capacità di controllo. Per questo, come osservato anche nell'intervista citata, le norme «non semplificano gli audit e la supervisione delle infrastrutture esterne», lasciando in parte irrisolta la questione del monitoraggio effettivo dei provider.

Sotto un profilo più ampio, il limite dell'approccio europeo risiede nella sua natura esclusivamente regolatoria e non industriale, caratterizzata da pochi investimenti su infrastrutture e piattaforme pubbliche, e relativa limitata capacità di calcolo. In mancanza di tali condizioni, la sola regolazione può mitigare i rischi, ma difficilmente elimina le cause profonde della dipendenza.

Anche le iniziative infrastrutturali nazionali, come il Polo Strategico Nazionale, pur rappresentando un avanzamento rispetto alla sola regolazione, essendo un tentativo di intervento sul controllo delle infrastrutture, non risolvono integralmente la questione della sovranità digitale. La sua architettura prevede un rafforzamento della localizzazione dei dati e della governance pubblica, ma integrando anche componenti tecnologiche e servizi sviluppati da attori privati globali, elementi che possono compromettere l'indipendenza infrastrutturale. Inoltre, la centralizzazione nazionale del sistema comporta una concentrazione dei dati, che pur favorendo il controllo e la standardizzazione, solleva interrogativi sulla possibilità di diversificazione e sull'interoperabilità a livello europeo. In tal senso, il PSN non costituisce una soluzione definitiva al problema delle dipendenze tecnologiche strutturali, ponendo il tema della necessità di coordinamento e progettualità su scala europea.

Tutte queste valutazioni non implicano una svalutazione del percorso fatto dall'Europa. Al contrario, il quadro normativo europeo è uno dei tentativi più avanzati di governo della trasformazione digitale. Tuttavia, la sfida della sovranità digitale è tanto ampia da andare oltre il tema della norma: non solo regolare l'uso delle tecnologie, ma anche incidere sulla loro produzione, controllo e distribuzione.

In conclusione, questo approccio, pur significativo, non risulta sufficiente per rispondere al problema. Esso rafforza la sicurezza, disciplina la circolazione dei dati e introduce meccanismi di portabilità e certificazione, ma non agisce sull'infrastruttura che è il nucleo della dipendenza. Per questo motivo si ritiene necessario integrare queste norme con una soluzione operativa. Nel prossimo capitolo infatti indagheremo il progetto GAIA-X, iniziativa europea

volta a sviluppare un'infrastruttura federata dei dati, concepita come progetto tecnologico per tradurre l'ambizione della sovranità digitale nella realtà.

Capitolo 3

GAIA-X come progetto di sovranità dei dati

Introduzione

L'analisi condotta nei capitoli precedenti ha mostrato come la sovranità digitale non possa essere intesa come esclusiva questione normativa o di sicurezza informatica, ma anche come problema strutturale legato al controllo delle infrastrutture e delle condizioni di utilizzo dei dati. Inoltre, nell'analisi della Strategia Europea per i Dati è emerso come uno degli obiettivi dell'Unione sia la costruzione di un mercato unico europeo, fondato su regole comuni, per permettere la condivisione sicura delle informazioni. Per rispondere a queste esigenze si rende necessario tradurre tali principi in configurazioni operative. In questo contesto si colloca GAIA-X, iniziativa promossa a livello europeo con l'obiettivo di costruire un ecosistema federato di dati e servizi cloud fondato su regole comuni, interoperabilità e meccanismi di fiducia verificabili. Il progetto propone di superare la frammentazione del mercato europeo e di ridurre le dipendenze strutturali da attori globali, mediante la definizione di un'architettura di standard condivisi.

Il capitolo analizzerà il contesto della nascita di GAIA-X e gli obiettivi strategici che propone. Successivamente verrà esaminata l'architettura tecnica dell'ecosistema, al fine di comprendere come la sovranità venga incorporata nella struttura stessa del sistema, con particolare attenzione ai meccanismi di Self-Description, Trust Framework e servizi federativi. Infine, verranno valutati risultati e limiti del progetto, analizzando studi e ricerche, ma integrando anche l'opinione di un esperto del settore, al fine di interrogarsi sull'effettiva capacità di incidere sugli equilibri del mercato cloud europeo e di riequilibrare le asimmetrie tra Stati e piattaforme.

3.1 Nascita di GAIA-X: contesto, obiettivi e principi

L'analisi condotta nel secondo capitolo ha messo in luce come il tema della sovranità digitale sia centrale per l'Unione Europea. Sebbene l'impianto regolatorio costruito sia solido per disciplinare la sicurezza e la circolazione dei dati, è emerso come, sul piano politico e strategico, la sovranità non possa limitarsi alla sola dimensione giuridica. Essa necessita, per

essere effettiva, di una dimensione operativa basata sul controllo di infrastrutture fisiche, servizi e standard, gestiti attualmente da attori privati. In questo contesto, nonostante iniziative come il Polo Strategico Nazionale (PSN), la necessità di garantire un controllo effettivo e l'interoperabilità dei dati richiede una soluzione di portata europea, che superi la frammentazione dei singoli stati. Partendo da queste criticità, il progetto GAIA-X si configura come il principale tentativo di risposta in capo all'Europa.

Per comprendere la nascita di GAIA-X è necessario esaminare il contesto in cui si colloca il documento della "Strategia Europea per i Dati", presentato dalla Commissione Europea per la creazione di un mercato europeo dei dati nel 2020. Oltre a favorire la circolazione dei dati, tale strategia, mira a costruire un ecosistema digitale basato sui valori di trasparenza, tutela della privacy e controllo democratico delle infrastrutture. In questo quadro, la sovranità viene concepita come la capacità effettiva di uno stato di esercitare pieno controllo nell'ambiente digitale, attraverso l'adozione di regole comuni e la gestione dei dati secondo standard condivisi.

È in questo contesto che si inserisce GAIA-X, inizialmente promossa nel 2019 dal Ministero federale tedesco dell'Economia e dell'Energia (BMWi) e dal Ministero francese dell'Economia e delle Finanze, come iniziativa politico-industriale volta a rafforzare l'autonomia strategica europea nel settore dei dati e del cloud. Tuttavia, fin dalle fasi iniziali, l'obiettivo era quello di superare la dimensione nazionale e costruire un sistema aperto e partecipato da tutti i componenti dell'UE.

Tale evoluzione si concretizza nel 2020 con la costituzione di Gaia-X European Association for Data and Cloud AISBL, associazione internazionale senza scopo di lucro con sede a Bruxelles, incaricata di definire la governance, gli standard e le specifiche del progetto[58]. A partire da questo momento assume una dimensione europea, coinvolgendo ad oggi nel 2026 oltre 250 membri in 25 paesi, articolandosi in 19 Hub europei e numerosi ecosistemi settoriali, anche al di fuori dell'Unione Europea[59]. L'obiettivo dichiarato è la creazione di un'infrastruttura dati e cloud federata, aperta e conforme ai valori europei, così come affermato nell'Architecture Document, documento tecnico ufficiale che definisce l'impianto concettuale e architetturale del progetto, «Gaia-X aims to create a federated open data infrastructure

[58] S. Autolitano, A. Pawlowska, *Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study,* IAI Papers 21|14, Istituto Affari Internazionali, 2021, pp. 12-13.
[59] Gaia-X European Association for Data and Cloud AISBL, *Gaia-X 2025 – Insieme verso un'infrastruttura dati federata e sicura*, Bruxelles, 2025, p. 3.

based on European values regarding data and cloud sovereignty»[60]. Tale formulazione è significativa perché chiarisce fin da subito che GAIA-X non è pensata come un nuovo provider europeo, o una nuova entità centralizzata, ma come un'architettura standard capace di federare infrastrutture e servizi esistenti e privati sotto un insieme di regole comuni. Dunque, il progetto rappresenta, il tentativo di tradurre in protocolli tecnici e operativi gli obiettivi definiti nella Strategia europea per i dati, definendo lo standard dell'architettura attraverso cui i servizi cloud possano interagire e risultare conformi a criteri di governance dei dati e fiducia.

A livello pratico, GAIA-X agisce come un framework europeo di coordinamento tecnico e normativo, volto a stabilire standard comuni, criteri di conformità e principi. Essa si configura come un livello di astrazione trasversale volto a stabilire regole e specifiche condivise, che permettono l'interazione tra molteplici attori.

La portata tecnica di questo progetto emerge ulteriormente nel documento architetturale, dove GAIA-X è descritta come un modello che federa ecosistemi indipendenti e autonomi, di proprietà di provider differenti. Come sottolineato nel testo: «There is one Gaia-X Ecosystem federating independent autonomous existing and future ecosystems»[61], che vengono collegati tramite protocolli e specifiche condivise. L'unità dell'architettura non deriva quindi da una centralizzazione infrastrutturale, ma dall'adozione condivisa di specifiche interoperabili. In quest'ottica, la federazione si configura come un principio architetturale ancor prima che politico, consentendo l'interconnessione di domini differenti mantenendo l'autonomia operativa dei singoli nodi.

Approfondendo il profilo tecnico, GAIA-X affronta il problema strutturale dell'ecosistema cloud europeo, colmando questo vuoto e fornendo gli strumenti per la gestione di servizi forniti da provider eterogenei, mitigando così il rischio di vendor lock-in. Tale impostazione permette di concretizzare gli obiettivi del progetto, che mirano a ridefinire le condizioni di funzionamento del sistema. In particolare, rendere strutturalmente possibile l'interazione tra fornitori diversi, garantire trasparenza nelle condizioni di utilizzo dei dati e costruire un modello federato in grado di ridurre le dipendenze sistemiche.

[60] Gaia-X European Association for Data and Cloud AISBL, *Gaia-X Architecture Document 22.04 Release*, Gaia-X AISBL, 2022, p. 2.
[61] Ivi, p. 10.

Per affrontare tali questioni il progetto si basa su due concetti fondamentali: l'interoperabilità e la portabilità. Mentre la prima viene intesa come la capacità di sistemi o servizi multipli di scambiare e usare reciprocamente informazioni, la portabilità si configura invece come la possibilità di trasferire e processare servizi tra provider differenti senza alterare la qualità del servizio. Tali definizioni non sono esclusivamente teoriche ma presuppongono requisiti implementativi stringenti, come l'adozione di API standardizzate, l'impiego di formati descrittivi condivisi e meccanismi di autenticazione.

In questo senso, le Self Description rappresentano uno degli elementi cardine del progetto, ovvero rappresentazioni formalizzate degli attori e dei servizi da loro offerti, che vengono redatte secondo modelli condivisi e standardizzati per la lettura automatica. Esse sono dispositivi architetturali, funzionali alla rappresentazione di un ecosistema trasparente e verificabile. Il loro significato risiede nella funzione che svolgono, ovvero rendere espliciti attributi, condizioni di utilizzo, requisiti di conformità e caratteristiche operative in un formato interoperabile. In tal modo, l'informazione relativa al cloud cessa di essere opaca, e diviene un elemento strutturale dell'ecosistema.

La rilevanza di tale meccanismo va interpretata alla luce della definizione che GAIA-X propone riguardo alla sovranità digitale, ossia la capacità del proprietario del dato di esercitare controllo sulla locazione e sulle condizioni di utilizzo delle proprie risorse informative, come definito nel documento programmatico del Gaia-X Hub Deutschland «Data sovereignty grants data providers full control over their data and digital identities, with the power to control who uses their data, for what purposes, and under what conditions.»[62]. Le self-descriptions si inseriscono in modo preciso in questa logica, rendendo il controllo tecnicamente rappresentabile e verificabile. Ne consegue che, per GAIA-X la sovranità non è solo statuale o contrattuale, ma proprietà emergente di un'architettura che rende le condizioni d'uso esplicite, formalizzate e interoperabili.

Parallelamente a questo, il Trust Framework rappresenta il secondo pilastro teorico del progetto, dato che definisce l'insieme di regole e requisiti per poter partecipare a GAIA-X, stabilendo un livello di compatibilità tra i diversi attori. La sua funzione non è quella di sostituire le normative nazionali o sovranazionali, bensì tradurre i principi fondamentali in criteri strutturati, condivisi e applicabili in modo trasversale nei diversi settori. Come emerge nel

[62] Gaia-X Hub Deutschland c/o acatech, *Setting the course: Gaia-X and the future of data-centric government*, Gaia-X Hub Deutschland, 2024, p. 9.

documento architetturale, il Trust Framework viene definito come «the process of going through and validating the set of automatically enforceable rules to achieve the minimum level of Self-Description compatibility»[63], ovvero il dispositivo attraverso cui le regole e gli standard definiti nell'ecosistema assumono coerenza e uniformità, riducendo la frammentazione del mercato europeo.

In questo contesto, l'interoperabilità e la portabilità già richiamate negli obiettivi fondamentali, assumono una valenza sistemica. Non si tratta di garantire semplicemente la compatibilità dei servizi, ma costruire un ambiente in cui la migrazione e l'uso di provider differenti non compromettano la continuità operativa e la governabilità dei dati. Le definizioni attribuite a questi due concetti delineano il quadro entro cui la sovranità viene esercitata, non attraverso la chiusura, ma mediante l'effettiva possibilità di scelta e mobilità.

Da questa prospettiva, la federazione costruisce il proprio principio fondamentale, ovvero la creazione di un ecosistema in cui attori indipendenti cooperano secondo norme condivise. Inoltre, viene sottolineato come la decentralizzazione e la federazione contribuiscano ad aumentare la resilienza e la ridondanza, riducendo il rischio di concentrazione del potere tecnologico. La scelta politica dell'architettura viene riflettuta nella sua impostazione, che punta ad evitare la dipendenza da singoli nodi dominanti e a promuovere una struttura reticolare, nella quale la fiducia non venga monopolizzata da pochi attori.

Anche la fiducia viene trattata come una proprietà strutturale del sistema. Infatti, l'uso di meccanismi comuni per la definizione dei requisiti minimi di conformità e per attestare il rispetto di questi, si inseriscono in una più ampia strategia di costruzione del "web of trust", in linea con quanto detto nel documento "Technical Architecture", che costituisce uno dei primi testi di riferimento sull'impianto tecnico del progetto, «Federation technically enables connections and a Web of Trust between different (distributed, decentralized) parts of the ecosystem.»[64]. In tal modo, GAIA-X tenta di superare l'asimmetria informativa dei mercati digitali, in cui l'utente finale spesso non riesce a valutare le condizioni di trattamento dei propri dati, perché privo degli strumenti necessari.

La struttura multilivello della compliance in Gaia-X rivela una strategia a più livelli, che gestisce l'equilibrio tra l'esigenza di standard comuni e la necessità di flessibilità operativa.

[63] Gaia-X European Association for Data and Cloud AISBL, *Gaia-X Architecture Document 22.04 Release*, Gaia-X AISBL, 2022, p. 31.
[64] Federal Ministry for Economic Affairs and Energy, *GAIA-X: Technical Architecture*, BMWi, 2020, p. 26.

L’adozione di una base condivisa garantisce interoperabilità e coerenza, mentre la possibilità di ulteriori qualificazioni consente adattamenti a contesti settoriali specifici. In questa configurazione, la standardizzazione non si traduce in rigidità eccessiva, ma in un equilibrio tra esigenze regolative e dinamiche di mercato.

Alla luce di tali elementi, la nascita di GAIA-X appare come un tentativo di costruire un’infrastruttura di regole e standard, in cui la sovranità sia incorporata nell’architettura stessa dell’ecosistema dati europeo. L’obiettivo è definire un coordinamento comune capace di federare infrastrutture differenti sotto criteri comuni, senza sostituire gli attori esistenti. All’interno del quadro della Strategia Europea per i Dati, GAIA-X rappresenta la risposta alla frammentazione del mercato digitale europeo, che mira a rendere effettiva la sovranità dei dati senza ricorrere a forme di isolazionismo o chiusura del mercato.

3.2 Modello di sovranità dei dati proposto da GAIA-X

Una volta delineata l’idea del progetto e la sua configurazione come framework federato, occorre ora soffermarsi sul modello di sovranità digitale che GAIA-X propone. La questione non è solamente ideologica, ma presenta il centro politico dell’intera iniziativa, poiché il concetto di sovranità viene riformulato in termini di controllo sulle condizioni d’uso dei dati, trasferendo l’attenzione dal rispetto normativo al governo operativo delle policy in ecosistemi multi-provider.

Il tema della sovranità digitale ha spesso assunto, nel dibattito europeo, una pluralità di significati, che comprendono letture incentrate sulla localizzazione territoriale dei dati e approcci orientati al controllo fisico delle infrastrutture. A differenza però delle interpretazioni che la riducono alla sola localizzazione fisica, GAIA-X propone una definizione fondata sulla governabilità dei flussi informativi, che mira a rendere compatibili apertura e controllo, ponendo la sovranità sul piano delle condizioni d’accesso e d’uso anziché su quello del mero perimetro territoriale. Tale approccio emerge chiaramente nel documento programmatico “Setting the course: Gaia-X and the future of data-centric government”[65] già introdotto nella sezione precedente, dove la sovranità dei dati diventa sostanziale nella capacità operativa del cliente di vincolare l'accesso e le finalità d'uso attraverso criteri tecnici.

[65] Gaia-X Hub Deutschland c/o acatech, *Setting the course: Gaia-X and the future of data-centric government*, Gaia-X Hub Deutschland, 2024, p. 9.

Questa definizione non fa riferimento alla proprietà dell'infrastruttura, ma alla facoltà di far rispettare e definire le regole di utilizzo. Una distinzione simile trova riscontro anche nell'esperienza di operatori del settore. Nell'intervista fatta da chi scrive a Leonardo Lorenzetto, Presale Engineer & Solution Architect di un'azienda operante nel settore cloud per la PA[66], emerge come la sovranità digitale difficilmente possa essere interpretata oggi come piena autonomia tecnologica. Questo perché anche se i dati sono localizzati in Europa, molte componenti dell'infrastruttura sono parte di filiere tecnologiche globali. Secondo l'intervistato, per questo motivo, ciò che può essere concretamente garantito è soprattutto una sovranità giuridica e operativa, ovvero la possibilità di stabilire con precisione «la localizzazione fisica del dato, la giurisdizione applicabile, i soggetti autorizzati all'accesso e i meccanismi di audit e tracciabilità». Questa osservazione conferma come la sovranità digitale venga progressivamente reinterpretata non come autosufficienza tecnologica, ma come capacità di definire e far rispettare le condizioni di utilizzo dei dati. Tale modello permette l'inclusione di attori globali a patto che questi aderiscano a un framework di regole, superando la logica dell'esclusione a favore di quella della conformità. Si passa dunque da una sovranità di possesso a una sovranità di controllo procedurale, intesa come «control over one's own digital data, as well as self determination in the use and design of digital systems and processes»[67], coerentemente con quanto analizzato nella ricerca pubblicata in un paper dell'Istituto di Affari Internazionali, dove Gaia-X viene analizzata come caso studio della sovranità digitale europea.

L'impostazione definita implica un cambio di paradigma rispetto alla concezione tradizionale stato-centrica della sovranità, dato che nel contesto digitale essa deve confrontarsi con architetture distribuite, supply chain e servizi erogati da fornitori globali. GAIA-X riconosce queste complessità e costruisce un modello che mira a reintrodurre margini di controllo all'interno di sistemi distribuiti.

Il cuore del modello può essere diviso in tre dimensioni fondamentali per affrontare la sovranità: il controllo sulle policy, l'effettiva capacità di scelta e mobilità tra i servizi e infine

[66] Intervista realizzata dall'autore in data 27 febbraio 2026 a Leonardo Lorenzetto, Presale Engineer & Solution Architect di un'azienda operante nel settore cloud per la Pubblica Amministrazione. Trascrizione integrale disponibile in Appendice 3.
[67] S. Autolitano, A. Pawlowska, *Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study,* IAI Papers 21|14, Istituto Affari Internazionali, 2021, p. 3.

la standardizzazione delle condizioni contrattuali. Tale articolazione sintetizza gli elementi ricorrenti nei documenti programmatici e di compliance dell'iniziativa.

La prima dimensione – quella del controllo sulle policy – riguarda la definizione delle condizioni di utilizzo dei dati. Nel modello GAIA-X, i provider devono specificare in modo chiaro le modalità di accesso, i vincoli di trattamento, le finalità conseguite e i limiti temporali. La sovranità diviene quindi un concetto concreto, traducendosi nella possibilità di associare alle risorse regole esplicite. Questo aspetto assume una rilevanza particolare nei contesti dove la condivisione delle informazioni deve avvenire in modo controllato, evitando usi non autorizzati, come nel settore pubblico al centro della nostra analisi, garantendo che la circolazione delle informazioni non comporti mai perdita di governance. Tale impostazione rispecchia quanto indicato nel documento Gaia-X Policy Rules and Labelling Framework[68], in cui vengono definiti i requisiti di conformità che i fornitori devono rispettare, in particolare «the rights of the parties to use the service and any data therein», vincolando l'operato del provider alle istruzioni impartite dal cliente ovvero l'essere «ultimately bound to instructions of the customer».

Parallelamente, la seconda dimensione – l'effettiva capacità di scelta e mobilità tra i servizi – è strettamente connessa al problema del vendor lock-in, già individuato come criticità strutturale, che viene affrontato ora non solo come limite tecnico, ma anche come ostacolo all'autodeterminazione politica dell'utente. In questo senso, la possibilità di migrare, combinare o sostituire servizi senza perdere il controllo sui dati o sulle condizioni di utilizzo è garantita dalla sovranità. L'obiettivo dichiarato, infatti, è la realizzazione di un ecosistema capace di prevenire fenomeni di dipendenza tecnologica, garantendo fiducia ed elevati standard di protezione dei dati «implement an open ecosystem which avoids lock-in effects, provides trust and fulfills highest data privacy standards»[69]. In quest'ottica, i concetti di interoperabilità e portabilità, introdotti precedentemente, assumono una valenza politica. Il primo trasforma l'autodeterminazione da principio astratto in un effettivo potere di uscita, mentre il secondo garantisce all'utente la reversibilità delle proprie scelte.

In tale prospettiva, la sovranità si configura anche come diritto di recesso, inteso non soltanto come possibilità di migrare tra servizi, ma anche come facoltà di rinegoziare i rapporti

[68] Gaia-X European Association for Data and Cloud AISBL, *Gaia-X Policy Rules and Labelling Document Release 22.04,* Gaia-X AISBL, 2022, p. 4.
[69] Federal Ministry for Economic Affairs and Energy, *GAIA-X: Technical Architecture*, BMWi, 2020, p. 32.

contrattuali con un provider. In mercati caratterizzati da forti economie di scala e di rete, l'esistenza formale di più alternative non basta. Ciò che conta è che il fornitore percepisca come concreta e realizzabile la possibilità di essere sostituito. Il modello punta a rafforzare la posizione dell'utente, attraverso condizioni che rendano possibile la mobilità e ridefiniscano i rapporti di potere tra domanda e offerta.

La terza dimensione – la standardizzazione delle condizioni contrattuali –, infine, riguarda la necessità di incorporare i principi generali in standard verificabili e condivisi. In tal senso, la sovranità non può essere garantita da semplici dichiarazioni di conformità, ma dalla possibilità di rappresentare e controllare in modo strutturato le condizioni di interazione. Come chiarisce il Compliance Document, documento che traduce i principi dell'iniziativa in criteri verificabili,

> «Permissible Standards shall identify standards respectively requirements/controls within such standards, where implementation shall be considered prima facie evidence of conformity with the related Gaia-X criterion».[70]

Richiamando il concetto di «code is law»[71] l'architettura diventa uno strumento di implementazione delle regole, trasformando le tutele giuridiche in requisiti tecnici automatizzati.

Sotto questo aspetto, la sovranità coincide con un aumento dell'accountability sistemica, ovvero la capacità dell'intero sistema di rendere le condizioni di utilizzo non soltanto dichiarate, ma strutturalmente confrontabili e verificabili. La trasparenza assume quindi una dimensione operativa, traducendo le policy in criteri comparabili che rendono ogni decisione consapevole e tecnicamente soggetta a controllo. In questa prospettiva, la sovranità assume la funzione di verifica delle regole più che della titolarità formale delle risorse. Tale impostazione trova riscontro nel dibattito europeo, dove la sovranità viene descritta come un concetto che «also entails regulatory and political elements»[72], evidenziando come il controllo si eserciti attraverso l'architettura delle regole.

Un ulteriore elemento qualificante è la dimensione collettiva di GAIA-X. Infatti, la sovranità non viene concepita come prerogativa dello stato singolo, ma come una proprietà emergente

[70] Gaia-X European Association for Data and Cloud AISBL, *Gaia-X Compliance Document*, Gaia-X AISBL, 2024, p. 6.
[71] L. Lessig (1999), *Code and Other Laws of Cyberspace*, New York, Basic Books, pp. 13-37.
[72] S. Autolitano, A. Pawlowska, *Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study,* IAI Papers 21|14, Istituto Affari Internazionali, 2021, p. 4.

di un ecosistema in cui attori pubblici e privati cooperano. Per questo motivo la forma di governance che viene proposta è articolata in hub nazionali e gruppi di lavoro tematici.

È importante quindi sottolineare come la capacità effettiva di incidere sui rapporti tra stato e piattaforme dipende dall'adozione concreta degli standard e dalla partecipazione degli operatori. Tuttavia, il progetto introduce in ogni caso un quadro di riferimento che consente di trasformare la sovranità da aspirazione politica a configurazione tecnica.

Dal confronto con altri modelli è possibile chiarire ulteriormente la specificità dell'approccio GAIA-X. Nel caso del Polo Strategico Nazionale, la sovranità viene perseguita attraverso il controllo e localizzazione dei dati su infrastrutture qualificate controllate dalla pubblica amministrazione. Mentre tale modello garantisce la sicurezza mediante la gestione dei dati sensibili internamente al perimetro nazionale, GAIA-X punta a costruire un ecosistema dove il controllo non dipende dalla posizione fisica del server, ma dall'adozione di standard che proteggono i dati anche in mercati aperti.

Analogamente, rispetto all'attuale modello dominante, dove «Europe's digital infrastructure currently lies in the hands of a small number of major non-European corporations»[73], e dove dunque le condizioni sono spesso determinate dai fornitori, viene proposta con GAIA-X una logica di simmetria informativa e comparabilità. La sovranità, in questo contesto, riduce l'opacità contrattuale perché consente di valutare e confrontare i servizi sulla base di criteri comuni.

In conclusione, il modello di sovranità dei dati proposto da GAIA-X può essere descritto come un tentativo di coniugare apertura del mercato e controllo strutturato, evitando sia il protezionismo tecnologico sia la dipendenza passiva da attori dominanti. La sovranità è dunque una proprietà che emerge dall'interazione tra architettura tecnica, governance e regole condivise. Nel prossimo paragrafo verrà fatta un'analisi dell'architettura e del funzionamento tecnico dell'ecosistema, in cui sarà possibile valutare in che misura gli strumenti predisposti da GAIA-X siano idonei a tradurre tale modello in pratica operativa.

3.3 Architettura di GAIA-X e funzionamento tecnico dell'ecosistema

L'analisi della sovranità svolta in precedenza trova la sua applicazione esaminando il funzionamento tecnico dell'ecosistema. Riprendendo l'Architecture Document, la struttura di

[73] Ivi, p. 13.

GAIA-X viene più volte definita come uno strato logico di servizi federativi, che agiscono a un livello superiore rispetto ai provider esistenti. L'obiettivo è ora analizzare come tale architettura traduca i principi di controllo in standard operativi.

Per comprendere come questa federazione si costituisce, è utile partire dal modello concettuale su cui si basa GAIA-X. L'Architecture Document descrive un sistema composto da partecipanti, che possono assumere i ruoli di provider, consumer e federator e che interagiscono attraverso risorse e offerte di servizio[74]. La distinzione tra risorse fisiche, virtuali e virtuali istanziate è rilevante perché consente di rappresentare, nello stesso linguaggio descrittivo, sia asset statici (dataset, configurazioni, licenze, modelli) che servizi run-time con endpoint e diritti di accesso. In altri termini, GAIA-X non standardizza "che cosa" debba essere un servizio cloud, ma "come" quel servizio debba essere esprimibile e confrontabile. Sotto questo profilo, la federazione non nasce dall'omogeneità dell'infrastruttura sottostante, ma dalla standardizzazione del modo in cui tali entità vengono descritte, identificate e collegate a regole d'uso.

L'elemento centrale che rende possibile questo "strato comune" è rappresentato dalle Self-Description, ovvero artefatti machine-readable che descrivono in forma interpretabile le entità definite nel modello concettuale (partecipanti, risorse, servizi) e che incorporano asserzioni verificabili. Come definite dal documento architetturale «Self-Descriptions in combination with trustworthy verification mechanisms empower Participants in their decision-making processes»[75]. Tali artefatti permettono quindi di alimentare i processi operativi oltre a quelli documentativi. Proprietà come la trasparenza vengono così ottenute rendendo formalizzabili e interrogabili attributi, policy e attestazioni, in modo che l'utente possa esprimere vincoli comparabili e il sistema possa supportare verifiche e automatismi.

Da un punto di vista tecnico le Self-Description non sono semplici file di testo, ma si configurano come un'architettura basata sullo standard W3C Verifiable Credentials (VC) e Presentations (VP). Nello specifico, una Credential è un'asserzione firmata digitalmente e quindi crittograficamente verificabile rispetto all'identità dell'issuer e all'integrità del contenuto, es. "questo server è in Italia". La Presentation rappresenta invece il pacchetto di una o più credenziali che il fornitore espone al sistema per dimostrare il possesso dei requisiti

[74] Gaia-X European Association for Data and Cloud AISBL, *Gaia-X Architecture Document 22.04 Release*, Gaia-X AISBL, 2022, pp. 12-14.
[75] Ivi, p. 20.

dichiarati.

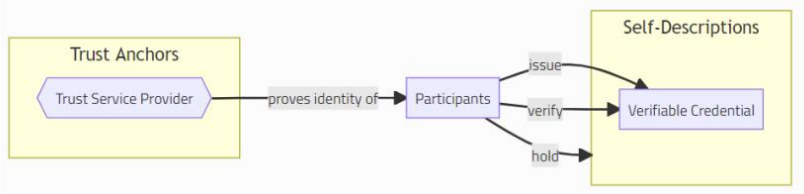

Figura 1: Trust Anchors, Participants e Verifiable Credentials nel Trust Framework.

Il meccanismo di relazione tra trust anchor, partecipante e credenziale verificabile è illustrato in figura 1, che schematizza la catena di fiducia su cui si fonda la validazione delle Self-Descriptions all'interno del Trust Framework Gaia-X.

Tali informazioni vengono serializzate in JSON-LD, un formato che permette di collegare i dati tra loro tramite linked data, eliminando ambiguità interpretative. La struttura logica adotta un modello RDF per poter rappresentare le informazioni come grafo di relazioni, rendendo l'ecosistema una rete di nodi e servizi interconnessi e interrogabili automaticamente[76]. Questo consente, da un lato, di far coesistere in una stessa Self-Description asserzioni provenienti da soggetti diversi (es. un provider dichiara certe proprietà tecniche, mentre un organismo terzo attesta questo requisito di conformità), preservando origine e integrità tramite firme e issuer distinti; dall'altro, abilita un approccio interrogabile e componibile in cui le informazioni hanno una struttura definita. Questa logica è coerente anche con il Trust Framework, il quale stabilisce i requisiti minimi per l'accesso al sistema e dichiara l'uso di attestazioni digitali verificate e di dati interconnessi (linked data) per costruire un grafo di conoscenza (knowledge graph) composto da asserzioni certificate, da cui possano essere computati indici automatici di fiducia e compatibilità. In linea con quanto descritto, il framework usa «verifiable credentials and linked data representation to build a FAIR knowledge graph of verifiable claims from which additional trust and composability indexes can be automatically computed»[77].

Affinché questo schema funzioni operativamente, però, è necessaria una catena di fiducia e un insieme di servizi federativi, che rendano le Self-Description e le relative credenziali utilizzabili nel ciclo di vita reale di un servizio nell'ecosistema. In questo contesto intervengono

[76] Ivi, pp. 20-25.
[77] Gaia-X European Association for Data and Cloud AISBL, *Gaia-X Trust Framework - 22.04 Release*, Gaia-X AISBL, 2022, p. 3.

i Federation Services (GXFS), intesi sia come un riferimento architetturale, sia come un insieme di strumenti per implementare funzioni e interfacce necessarie alla federazione. Essi costituiscono un riferimento architetturale, le cui implementazioni concrete possono variare tra ecosistemi, purché rispettino le funzioni previste e le interfacce di interoperabilità definite dal framework. Questo principio è esplicitato nel documento dedicato ai Federation Services, il quale sottolinea la natura adattabile di tali strumenti. Poiché i requisiti operativi possono divergere sensibilmente tra diverse federazioni settoriali, i partecipanti conservano la facoltà di sviluppare servizi e interfacce personalizzati per il proprio contesto. Questa flessibilità è garantita dalla promozione dell'approccio open source, per permettere lo sviluppo di funzioni necessarie, pur mantenendo la compatibilità con gli standard comuni[78].

Questa architettura può essere tradotta in una struttura operativa ricostruendo l'ecosistema come un insieme di componenti funzionali che agiscono sinergicamente. GAIA-X articola i propri servizi attorno a dei concetti fondamentali, a partire dallo strato *Identity & Trust*, responsabile della gestione delle identità digitali e delle credenziali verificate. Su questa base di fiducia si innesta il *Federated Catalogue*, che permette di visualizzare e selezionare le offerte del sistema sulla base della validazione delle Self-Descriptions[79]. La fase esecutiva viene affidata poi ai servizi di *Sovereign Data Exchange*, che regolano la negoziazione contrattuale e il tracciamento delle transazioni, garantendo che gli scambi avvengano nel rispetto delle policy. Tutto questo apparato è monitorato dai servizi di *Compliance & Registry*, che assicurano la verifica dei requisiti rispetto a registri di fiducia, mentre lo strato di *Portals and APIs* garantisce l'interazione tra i partecipanti attraverso interfacce coerenti. Tale struttura delinea le componenti strutturali necessarie a garantire il controllo e la verificabilità delle condizioni d'uso dei dati, definendo poi un flusso operativo per generare fiducia tra gli attori. Essa può essere illustrata come in figura 2, dove l'Architecture Docuement descrive Gaia-X come un sistema multilivello in cui i vari strati operano in modo integrato tra infrastruttura ed ecosistema.

[78] Gaia-X European Association for Data and Cloud AISBL, *Gaia-X Federation Services (GXFS)*, Gaia-X AISBL, 2021, p. 4-6.
[79] Gaia-X European Association for Data and Cloud AISBL, *Gaia-X Architecture Document 22.04 Release*, Gaia-X AISBL, 2022, p. 43.

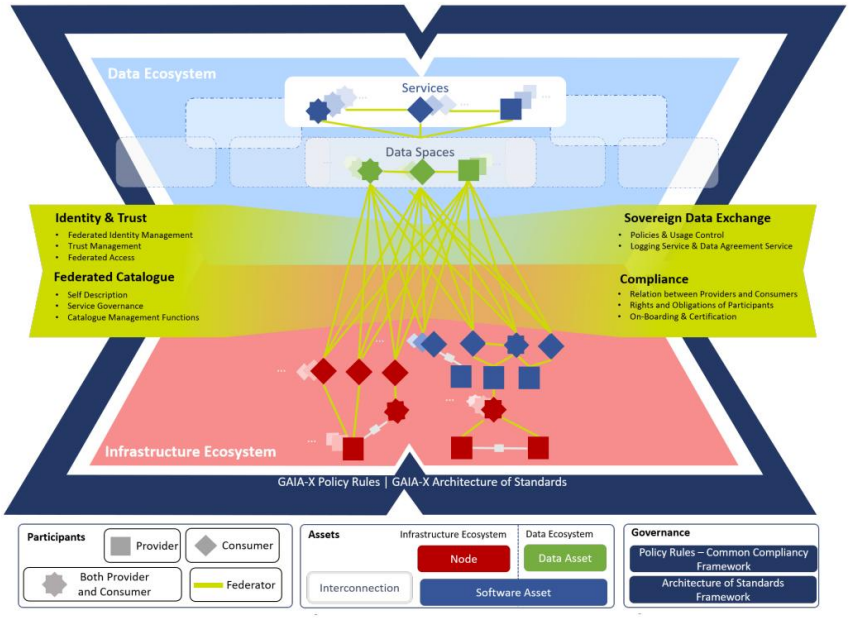

Figura 2: Componenti federativi e flusso operativo nell'architettura Gaia-X

L'analisi di questa architettura funzionale sposta l'attenzione verso l'effettiva implementazione dei suoi principi nei contesti reali. Lo studio tecnico svolto da Marta Zorrilla e Juan Yebenes, ricercatori di Big data technologies, Data Science e Data Governance presso l'Università della Cantabria[80], ha evidenziato come il framework, pur definendo i pilastri della federazione, non fornisca ancora una definizione completa delle modalità operative di gestione; gli autori osservano infatti che «there is no framework to guide the construction of an enterprise architecture for implementing data governance in DG in DSs». Ciò suggerisce che strumenti come Self-Description e Trust Framework rappresentano condizioni importanti per l'interoperabilità e la trasparenza, ma non sono di per sé sufficienti a garantire una piena operatività dei modelli di governance dei dati.

Una volta definiti i componenti architettonici e le loro criticità operative, è necessario definire come questi interagiscano per dare vita al flusso operativo della federazione in esercizio. Tale processo può essere descritto come una sequenza di fasi, in cui ogni passaggio traduce i principi astratti di sovranità in un ciclo di vita reale del servizio.

[80] M. Zorrilla, J. Yebenes, *Architecture Building Blocks for Data Governance in Data Spaces, in Information*, https://www.mdpi.com/2078-2489/16/11/927, ultimo accesso marzo 2026.

In primo luogo, il fornitore che desidera partecipare a GAIA-X deve generare la Self-Description della propria offerta, includendo claim rilevanti, siano essi autodichiarati o attestati da terzi. In secondo luogo, le asserzioni devono essere firmate e collegate a un'identità verificabile, attraverso validazione crittografica di firme e mittenti. In questo passaggio risiede la centralità dei trust anchors e delle regole del Trust Framework dato che «all keypairs used to sign claims must have at least one of the Trust Anchor in their certificate chain»[81]. Il Trust Framework e i trust anchors definiscono infatti gli standard di sintassi, serializzazione e coerenza necessari a garantire la veridicità dei dati. Prima della pubblicazione, la Self Description è validata rispetto a schemi, firme e catene di fiducia, così che il catalogo indicizzi descrizioni già verificabili e semanticamente conformi. Successivamente, viene pubblicata nel Federated Catalogue, ovvero il repository indicizzato che abilita la ricerca e la selezione dei fornitori su scala federata.

Invece, lato consumatore, la ricerca avviene tramite filtri su metadati strutturati: l'utente esprime vincoli precisi (come giurisdizione, policy…) e ottiene offerte confrontabili proprio perché rese disponibili in forma machine-readable. Una volta identificata l'offerta, si apre la fase di negoziazione ed entra in gioco il Contract/Service Agreement Service, servizio che abilita una transazione sicura e verificabile offrendo interfacce di negoziazione dei termini. L'Architecture Document approfondisce questa fase, richiamando il concetto di "computable contracts" volti a supportare il design e la negoziazione contrattuale al fine di «observe the fulfillment of contractual obligations and compliance with national law»[82]. In questa cornice, l'idea dei "computable contracts" deve essere intesa come un orientamento architetturale a rendere i termini dello scambio più osservabili e verificabili lungo il ciclo di vita del servizio. Di conseguenza, le condizioni d'uso possono essere espresse in modo più strutturato e comparabile, mentre i servizi di data exchange e logging supportano la tracciabilità delle obbligazioni e degli eventi rilevanti ai fini di audit e accountability.

Durante la transazione vera e propria, il Contract Logging Service riceve i log necessari a tracciare l'erogazione del servizio e il rispetto delle politiche d'uso, segnalando eventuali anomalie, che restano accessibili anche successivamente per garantire la rendicontabilità.[83]

[81] Gaia-X European Association for Data and Cloud AISBL, *Gaia-X Trust Framework - 22.04 Release*, Gaia-X AISBL, 2022, p. 5.
[82] Gaia-X European Association for Data and Cloud AISBL, *Gaia-X Architecture Document 22.04 Release*, Gaia-X AISBL, 2022, p. 16.
[83] Ivi, pp. 16-17.

Qualora servano prove più forti, interviene la funzione di Compliance e Notarization: sia i documenti di labelling che il Compliance Document chiariscono che la validazione di un claim può essere rilasciata come credenziale verificata da organismi terzi accreditati nel registro[84]. Infine, l'interazione pratica con l'intero sistema è mediata da Portals and APIs, che supportano la manutenzione delle identità e la gestione delle offerte in coerenza con la natura decentralizzata del modello[85].

Possiamo comprendere, quindi, come l'architettura trasforma il concetto di sovranità in un controllo effettivo sulle condizioni d'uso, attraverso una concatenazione di attività. Alcuni studi tecnici, come la revisione sistematica sulla governance dei data spaces pubblicata sulla rivista Information[86], hanno tuttavia evidenziato che il modello architetturale proposto non fornisce ancora una definizione completa delle modalità operative con cui tali principi debbano essere implementati nei diversi ecosistemi applicativi. Viene infatti osservato che «GAIA-X does not provide a specific architecture for implementing data governance», evidenziando come il framework stabilisca standard e linee guida generali, ma lasci ancora aperta la definizione di alcune modalità concrete di implementazione. Questa osservazione teorica trova riscontro anche nella pratica operativa soprattutto in organizzazioni pubbliche con risorse tecniche limitate. L'esperienza pratica riportata nell'intervista già citata evidenzia come molte amministrazioni locali dispongano di competenze ICT ridotte o fortemente esternalizzate. Come osserva Lorenzetti in questi contesti «può risultare complesso far distinguere con precisione tra IaaS, PaaS e SaaS o far comprendere pienamente l'impatto infrastrutturale di determinate scelte». Ciò suggerisce che l'adozione di framework federativi complessi, potrebbe richiedere un rafforzamento delle competenze interne alla pubblica amministrazione o la definizione di linee guida operative più chiare. Il fatto che i documenti distinguano esplicitamente queste fasi è quindi significativo nel funzionamento degli exchange services, poiché mostra come GAIA-X tenti di ancorare il controllo e la governance dei dati a un processo verificabile e strutturato, piuttosto che a una semplice dichiarazione di conformità.

[84] Ivi, pp. 32-39.
[85] Ivi, pp. 5-7.
[86] M. Zorrilla, J. Yebenes, *Architecture Building Blocks for Data Governance in Data Spaces, in Information*, https://www.mdpi.com/2078-2489/16/11/927, ultimo accesso marzo 2026.

Per comprendere meglio il funzionamento del modello, possiamo considerare il caso di una Pubblica Amministrazione che debba acquisire un servizio di conservazione documentale. A causa dei vincoli normativi la PA richiede: la chiara identificazione delle responsabilità contrattuali, l'impegno del fornitore a operare esclusivamente secondo le istruzioni del cliente e la possibilità di effettuare audit sistematici sulle transazioni. Utilizzando GAIA-X questo processo viene strutturato e reso maggiormente trasparente, e può essere suddiviso in quattro fasi:

1) *Selezione*: la PA visualizza il catalogo federato e filtra le offerte che presentano nelle proprie Self-Descriptions i claims relativi ai requisiti desiderati. L'affidabilità di tali asserzioni è garantita da credenziali verificate emesse da enti certificatori riconosciuti.
2) *Vincoli operativi*: In una prima fase, la logica definita nel Policy Rules Document permette di ancorare il servizio a requisiti espliciti, ad esempio stabilisce che il fornitore debba essere formalmente vincolato alle istruzioni del cliente definendo le modalità tecniche (API o configurazioni) attraverso cui tali istruzioni vengono impartite.
3) *Esecuzione e trasparenza*: Una volta formalizzato l'accordo tramite il Contract/Service Agreement Service, è possibile iniziare con l'erogazione del servizio. Durante l'uso, il Contract Logging Service produce evidenze digitali sulla trasmissione dei dati e sull'osservanza delle politiche d'uso, riducendo l'asimmetria informativa tra provider e PA.
4) *Auditability*: Qualora la PA debba dimostrare la conformità del servizio, la Self-Description permette di risalire con precisione all'ente che ha validato ogni singolo requisito. Così come previsto dal Compliance Document, l'uso di verifiable credentials e di un registro federato degli issuer fidati rende la rendicontazione una verifica digitale immediata.

Da questo esempio è possibile comprendere come la federazione non sostituisca le scelte politiche della PA, ma rende controllabile ciò che prima era più complesso verificare.

Un ulteriore punto che aiuta a comprendere perché GAIA-X sia concepita come federazione è la gestione delle regole definite nel Trust Framework, usate come baseline estendibile e versionata in modo automatico, in linea con quanto descritto nell'Architecture Document. Inoltre, il Compliance Document specifica da un lato che l'adozione di standard riconosciuti "permissible" costituisce una presunzione di conformità rispetto ai criteri Gaia-X. Dall'altro,

pone l'accento sulla accessibilità e verificabilità delle evidenze di conformità "accessibility" e sulla permanenza dei requisiti nel tempo: la conformità è intesa come un attributo che deve restare valutabile e monitorabile durante l'intero ciclo di vita del servizio. Questo dettaglio è rilevante perché mostra come GAIA-X cerchi di evitare che la compliance si riduca a "dichiarazioni", le regole devono essere verificabili e riusabili.

A questo punto risulta utile confrontare l'architettura di GAIA-X con il modello italiano delineato attraverso il Polo Strategico Nazionale (PSN). La strategia su cui esso si basa, per attuare la trasformazione digitale della pubblica amministrazione, consiste in un processo di classificazione di dati e servizi, qualificazione dei fornitori e migrazione verso infrastrutture idonee sotto il profilo di sicurezza e conformità normativa. Secondo quanto descritto nella Strategia Cloud Italia[87], essa si articola infatti nelle linee di «Classificazione dei dati e dei servizi», «Qualificazione dei servizi cloud» e nella creazione del «Polo Strategico Nazionale (PSN)» infrastruttura nazionale per l'erogazione di servizi cloud. In tale impostazione, la sovranità viene perseguita tramite il controllo del perimetro infrastrutturale fisico: la strategia mira, infatti, a garantire che i dati della PA siano ospitati in ambienti localizzati e qualificati a livello nazionale, rafforzando il controllo diretto sulle risorse tecnologiche critiche e riducendo così la dipendenza tecnologica dall'estero.

GAIA-X, al contrario, propone un modello di sovranità regolativa e architetturale. Piuttosto che costruire nuove infrastrutture fisiche o competere direttamente con gli hyperscaler, il progetto europeo punta a definire un insieme di regole, standard e meccanismi di interoperabilità che rendano possibile governare l'uso dei dati anche in ecosistemi distribuiti e multi-provider. In questo senso, la sovranità è legata alla capacità di stabilire e far rispettare le condizioni di utilizzo dei dati attraverso strumenti tecnici e normativi, mirando a incidere profondamente sulle modalità di funzionamento del mercato.

Da questa prospettiva, la federazione proposta da GAIA-X non sostituisce le infrastrutture nazionali come il PSN, ma si colloca a un livello differente, definendo il quadro di interoperabilità e fiducia entro cui infrastrutture e servizi già esistenti possono operare.Sotto questo profilo, le due strategie a confronto possono essere interpretate come livelli diversi di una stessa politica. I framework federativi europei, come GAIA-X, operano sul piano della

[87]Dipartimento per la trasformazione digitale, *Strategia Cloud Italia - La strategia cloud per la Pubblica Amministrazione*, in Docs Italia, https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/stabile/4_la_strategia_cloud_per_la_pubblica_amministrazione.html, ultimo accesso marzo 2026.

governance, creando le condizioni affinché infrastrutture diverse possano cooperare all'interno di un mercato digitale europeo regolato. Mentre, infrastrutture nazionali, come il PSN, garantiscono il controllo diretto sui dati più sensibili e sulle funzioni critiche della pubblica amministrazione attraverso il controllo materiale dell'infrastruttura fisica. L'autonomia strategica europea potrebbe quindi emergere proprio dall'interazione di questi due livelli: da un lato il rafforzamento delle capacità infrastrutturali nazionali, dall'altro la definizione di standard comuni che permettano l'interoperabilità tra ecosistemi diversi.

Nonostante le finalità convergenti, la loro differenza risiede nell'architettura scelta: nel caso del PSN, la sovranità è strettamente legata al controllo del luogo e delle condizioni di erogazione; invece, nel caso di GAIA-X, essa viene incorporata nella descrizione formale delle offerte, nella catena di fiducia delle credenziali e nei servizi federativi che rendono comparabili le condizioni d'uso. In termini comparativi, come osserva Mario Dal Co, Economista e manager, già direttore dell'Agenzia per l'innovazione:

> La fondamentale differenza tra il cloud federale e la soluzione adottata in Italia è la mancanza di intermediazione da parte di una società veicolo sulla quale è incardinato il contratto quadro. […] La differenza principale con la nostra esperienza consiste, quindi, nella volontà del governo federale di fare leva […] sulla capacità di collaborare delle Agenzie strategiche […]. Manca la società veicolo, che nel nostro Paese supplisce alla mancanza di capacità di gestire il procedimento di acquisto.[88]

Tale osservazione evidenzia come il modello italiano si fondi su un'architettura centralizzata, mentre il paradigma federale si basi su meccanismi di coordinamento distribuito.

Da un punto di vista tecnico, ciò significa che il PSN si fonda su una logica di qualificazione preventiva del fornitore e dell'infrastruttura, intervenendo a livello infrastrutturale e organizzativo, mentre GAIA-X introduce meccanismi di verificabilità continua basati su Self-Descriptions, Verifiable Credentials, Trust Framework e servizi di logging delle transazioni, agendo a livello semantico e federativo, cercando di rendere interoperabili domini diversi senza imporre un'unica piattaforma. Questo non implica una contrapposizione dei modelli, anzi potrebbero risultare teoricamente complementari. Un'infrastruttura qualificata a livello

[88] Mario Dal Co, *Polo strategico per il cloud, un errore puntare su un 'campione nazionale': ecco perché*, https://www.agendadigitale.eu/infrastrutture/polo-strategico-per-il-cloud-un-errore-puntare-su-un-campione-nazionale-ecco-perche/, ultimo accesso marzo 2026.

nazionale potrebbe adottare gli standard e i servizi federativi GAIA-X per rendere le proprie offerte interoperabili e verificabili su scala europea.

In tale prospettiva, GAIA-X non si limita a proporre un'infrastruttura "sovrana", ma ha l'ambizione più grande di ridefinire completamente il paradigma di governance dell'ecosistema cloud. Tuttavia, proprio la complessità di questo impianto solleva interrogativi sui costi di implementazione e sulla reale capacità di incidere sugli equilibri di mercato dominati da attori globali. Diviene infatti necessario valutare in che misura tale sistema riesca a produrre effetti concreti in termini di adozione, scalabilità e riduzione delle dipendenze sistemiche.

Proprio per mitigare i costi di implementazione e i rischi di dipendenza citati, alcuni studiosi hanno evidenziato anche il possibile ruolo che l'open source può avere nella costruzione di ecosistemi digitali più autonomi. A differenza dei modelli dominati da hyperscaler privati o da infrastrutture pubbliche centralizzate, l'open source può rappresentare una sorta di "terza via", fondata su modelli di sviluppo aperti, collaborativi e distribuiti. In tali contesti, la dipendenza dai singoli fornitori può essere ridotta, favorendo forme di governance più collegiali dell'infrastruttura digitale, rendendo codice, specifiche tecniche e strumenti software accessibili, verificabili e modificabili da una pluralità di attori.

Tale apertura non si esaurisce in una scelta puramente tecnica, ma si riflette in un nuovo paradigma di gestione delle risorse digitali, spesso identificato con il concetto di "digital commons", ovvero infrastrutture e risorse digitali gestite come beni comuni, secondo logiche collaborative e non proprietarie, attraverso processi di collaborazione tra istituzioni pubbliche, imprese e sviluppatori[89]. Come osservato nella letteratura sulla governance delle tecnologie digitali, i modelli open source possono contribuire a rafforzare la trasparenza, la sicurezza e la verificabilità dei sistemi, proprio perché il codice è aperto alla revisione pubblica e alla partecipazione di una comunità più ampia di soggetti.

Le istituzioni europee hanno riconosciuto l'importanza strategica dell'open source nel rafforzamento della sovranità digitale. Nello specifico, la Commissione Europea nel documento "Open Source Software Strategy 2020–2023" sottolinea come il software aperto possa contribuire all'autonomia tecnologica dell'Unione, osservando che «open source impacts the

[89] Treccani, *Creative Commons*, in Enciclopedia online, https://www.treccani.it/enciclopedia/creative-commons_(Lessico-del-XXI-Secolo), ultimo accesso marzo 2026.

digital autonomy of Europe»[90] e consente di creare e mantenere « its own, independent digital approach and stay in control of its processes, its information and its technology»[91]. In questa prospettiva, l'adozione di tecnologie open source non rappresenta soltanto una scelta tecnica, ma anche uno strumento di politica industriale e di autonomia strategica, poiché consente agli attori europei di sviluppare e controllare collettivamente parti rilevanti dell'ecosistema digitale. Sul piano architetturale, questa apertura si traduce nella possibilità di implementare standard condivisi tra diversi provider, facilitando l'interoperabilità effettiva tra ecosistemi differenti.

GAIA-X si inserisce parzialmente in questa logica, promuovendo l'uso di componenti open source e di specifiche tecniche aperte per lo sviluppo dei federation services e delle infrastrutture. Il framework mira a favorire la creazione di un ecosistema aperto, nel quale diversi attori possano contribuire allo sviluppo delle soluzioni tecniche e adattarle ai propri contesti applicativi, pur non essendo un progetto open source in senso stretto. In questo senso, l'approccio federativo e l'utilizzo di componenti aperti possono essere interpretati come un tentativo di combinare logiche di mercato, governance pubblica e modelli collaborativi di sviluppo tecnologico.

3.4 Limiti e risultati di GAIA-X

Dopo l'approfondimento sul funzionamento dell'ecosistema e della sua architettura è necessario interrogarsi sulla sua effettiva capacità di incidere sugli equilibri esistenti. Se nel paragrafo precedente è stato analizzato come GAIA-X abbia tradotto il concetto di sovranità digitale in operatività, resta ora da comprendere fino a che punto il modello abbia prodotto risultati concreti e quali siano, al contrario, i suoi limiti strutturali.

Il dibattito accademico e istituzionale sul tema evidenzia sin dall'inizio una tensione di fondo, e può essere analizzato riprendendo lo studio di Autolitano e Pawlowska. Le autrici sottolineano come il progetto rappresenti «a first important step in the right direction»[92] ma allo stesso tempo riconoscono che «it is certainly too early to assess whether the GAIA-X project will be successful or not»[93]. Tale prudenza riguarda la natura stessa dell'iniziativa,

[90] Commissione Europea, *Open Source Software Strategy 2020–2023*, in Comunicazioni della Commissione Europea, C (2020) 7149 final, 2020, p. 6.
[91] Ibidem.
[92] S. Autolitano, A. Pawlowska, *Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study,* IAI Papers 21|14, Istituto Affari Internazionali, 2021, p. 16.
[93] Ivi, p. 14.

che non nasce come alternativa al modello attuale, ma come quadro regolativo e tecnico capace di normare l'ecosistema cloud entro parametri di trasparenza, interoperabilità e controllo.

In un'intervista pubblicata dall'AI Now Institute[94] viene inoltre evidenziato come, fin dalle prime fasi, il progetto abbia sofferto di una certa ambiguità sugli obiettivi strategici. L'ex CEO dell'associazione Gaia-X Francesco Bonfiglio osserva infatti che «the ambitions of Gaia-X were big, but the clarity on the scope was not shared across all members», dato che i diversi attori avevano aspettative differenti dal progetto: alcuni lo immaginavano come un nuovo hyperscaler europeo, altri come un organismo di standardizzazione o come uno strumento politico per limitare il potere dei grandi provider. Questa pluralità di visioni ha contribuito a rendere più complessa la definizione di una strategia condivisa e coerente nel processo di sviluppo dell'iniziativa.

Oltre alla visione iniziale di un 'cloud europeo sovrano', molti studi di settore hanno osservato che si può delineare l'evoluzione di GAIA-X come un avanzato framework di standard e governance, piuttosto che come un'infrastruttura industriale destinata alla competizione diretta con gli hyperscaler globali. In questa direzione, Antonio Cisternino, ricercatore informatico e CIO dell'Università di Pisa, ha evidenziato che la sola standardizzazione di un'infrastruttura multi-cloud «non è vista come sufficiente a garantire un mercato capace di sostenere la formazione di player europei»[95] e che la partecipazione di giganti del cloud (come Google o AWS) può portare ad una situazione dove le regole vengono definite da chi già detiene il potere di mercato, senza modificare la struttura competitiva esistente. L'obiettivo qui non è negare l'utilità degli standard, ma sottolineare la difficoltà di far convergere interessi molto diversi all'interno di un unico ecosistema federato.

Questa difficoltà emerge in modo chiaro se analizziamo il costo complessivo di adozione. Anche in presenza di un'architettura aperta e multi-cloud, la scelta non si basa solo sul costo nominale del servizio, ma sul TCO (total cost of ownership), che comprende costi di migrazione e re-ingegnerizzazione applicativa, integrazione con sistemi esistenti, formazione e

[94] M. Scott, F. Bonfiglio, *Why Europe's Cloud Ambitions Have Failed, in Redirecting Europe's AI Industrial Policy*, AI Now Institute, https://ainowinstitute.org/publications/xi-why-europes-cloud-ambitions-have-failed, ultimo accesso marzo 2026.
[95] A. Cisternino, *Gaia-X, in crisi il cloud europeo? Le sfide da superare, con l'ingerenza delle big tech*, in Agenda Digitale, https://www.agendadigitale.eu/infrastrutture/gaia-x-anatomia-di-un-cloud-le-sfide-delleuropa-e-lingerenza-delle-big-tech/, ultimo accesso marzo 2026.

competenze, gestione operativa e, soprattutto, costi di uscita (exit) legati a dipendenze tecniche e contrattuali. In questa prospettiva, l'obiettivo di realizzare l'interoperabilità va letto come tentativo di ridurre i componenti strutturali del TCO che, nel mercato reale, diventano i principali problemi di lock-in. Un'analisi svolta da Federica Maria Rita Livelli, Business Continuity & Risk Management Consultant, sottolinea infatti che il confronto tra "cloud sovrano" e hyperscaler va affrontato considerando l'intero costo di ciclo di vita, includendo gli oneri di governance, migrazione e gestione del rischio, dato che «un confronto limitato ai soli costi infrastrutturali risulta insufficiente e potenzialmente fuorviante. Il TCO deve includere compliance normativa, rischio regolatorio, lock-in tecnologico, portabilità futura, competenze, supporto operativo e sostenibilità»[96].

Dal punto di vista progettuale, la questione del lock-in non è solo teorica, come riportato dall'intervista fatta, l'esperto distingue chiaramente tra livello infrastrutturale e livello applicativo: se a livello IaaS la standardizzazione rende tecnicamente possibile replicare un'architettura presso un altro provider, a livello PaaS e SaaS la dipendenza diventa organizzativa e procedurale, richiedendo revisione dei processi, formazione del personale e riconfigurazione delle integrazioni. Ciò conferma che la riduzione del lock-in dipende non solo dagli standard federativi, ma dalle scelte architetturali e contrattuali adottate in fase di progetto.

Al di là di queste criticità, un risultato importante di GAIA-X consiste nell'aver istituzionalizzato la sovranità digitale in un linguaggio tecnico-normativo condiviso. Il progetto ha contribuito a dare corpo a concetti come interoperabilità, portabilità e trasparenza contrattuale, che oggi compaiono sempre più spesso nei requisiti dei bandi di gara pubblici, o nelle richieste di aziende private. Anche fonti istituzionali, come il BMWi tedesco, riconoscono la creazione di un "ecosistema infrastrutturale" cloud fondato sui valori dell'Unione, essenziali per competere all'interno del mercato unico digitale europeo. In questo senso, anche se l'adozione operativa del framework non è ancora avvenuta, ha già imposto una disciplina tecnica a cui riferirsi. Tuttavia, deve essere ricordato che GAIA-X non introduce obblighi giuridici vincolanti per i partecipanti, ma si fonda su un'adesione volontaria e su meccanismi di autoregolazione. La capacità del progetto di incidere concretamente dipende dall'attrattività e dalla diffusione tra i vari attori privati. In assenza di una partecipazione significativa c'è il rischio che GAIA-X rimanga un riferimento formale e di basso impatto. Riprendendo

[96] F. M. R. Livelli, *Analisi del TCO (total cost of ownership): differenze tra cloud sovrano e hyperscaler*, in Agenda Digitale, https://www.agendadigitale.eu/procurement/analisi-del-tco-total-cost-of-ownership-differenze-tra-cloud-sovrano-e-hyperscaler/, ultimo accesso marzo 2026.

l'opinione di Lorenzetto, un framework non vincolante «dipende dalla sua capacità di generare valore percepito e vantaggio competitivo per gli operatori che decidono di aderirvi», e quindi l'effetto sugli equilibri di mercato sarà concreto solo se integrato stabilmente nelle politiche industriali e nei meccanismi di procurement europei.

Altro segnale tangibile è la diffusione di data spaces e hub nazionali, che operano come centri di competenza e diffusione, con progetti settoriali in ambiti come finanza, energia e automotive. A questo si affianca l'adesione di operatori industriali e cloud provider europei, come Aruba, che è "Day-1 Member" del progetto e hub nazionale per l'Italia. Il provider ha aderito con l'obiettivo di garantire interoperabilità tra operatori aderenti, sostenendo il nuovo standard europeo per la creazione e l'erogazione di servizi cloud e favorendo un ecosistema aperto in cui dati e servizi possono essere resi disponibili, raccolti e condivisi in un ambiente protetto[97]. L'esistenza di oltre 16 hub nazionali e centinaia di membri dell'associazione indica un forte interesse nel settore, risultato non trascurabile per un'iniziativa avviata solo da pochi anni.

Nonostante questi risultati, i limiti strutturali restano evidenti e sono al centro del dibattito. Uno dei temi più sentiti riguarda la competizione con gli hyperscaler globali. L'enorme concentrazione del mercato cloud in capo a pochi attori (stime recenti indicano che circa il 65 % del mercato europeo e globale del cloud è controllato da tre hyperscaler statunitensi[98]), crea barriere difficili da superare esclusivamente con standard federativi. Di conseguenza, la natura collaborativa di GAIA-X, che dalla prospettiva architetturale può essere un punto di forza, può diventare un limite dell'ambizione geopolitica, dato che la federazione da sola non crea attori capaci di competere con big statunitensi o cinesi. In altri termini, gli standard non possono annullare automaticamente i vantaggi di scala né le asimmetrie economiche che incidono sul TCO, come la disponibilità di servizi gestiti, gli incentivi di prezzo e i pacchetti commerciali che rendono conveniente l'entrata ma costosa l'uscita. In questo senso, il punto critico è tecnico e organizzativo: se il TCO resta più favorevole agli hyperscaler, la federazione rischia di rimanere un livello di governance che non sposta davvero gli equilibri

[97] Aruba, *Aruba favorisce lo sviluppo del cloud aperto e aderisce a GAIA-X,* in Aruba Magazine, https://www.aruba.it/magazine/cloud/aruba-favorisce-lo-sviluppo-del-cloud-aperto-e-aderisce-a-gaia-x.aspx, ultimo accesso marzo 2026.
[98] Gaia-X Association for Data and Cloud AISBL, *Market-X 2025 – Plenary Room*, Gaia-X AISBL, 2025, p. 5.

industriali.[99] A confermare questa visione è lo stesso Francesco Bonfiglio, il quale sottolinea come, nonostante le iniziative politiche e gli investimenti pubblici, «Europe's collective market share of the cloud computing industry has fallen»[100], segnalando che la posizione competitiva dei provider europei non si è rafforzata in modo significativo. Tale evidenza sottolinea il paradosso di un'Europa che, pur normando e standardizzando il settore, non riesce a invertire il trend di marginalizzazione dei propri provider rispetto a una struttura di mercato caratterizzata da forti economie di scala e da una concentrazione tecnologica già consolidata.

Le criticità emergono anche a livello operativo. La complessità delle regole e dei meccanismi di compliance, così come la necessità di competenze tecniche avanzate per interpretarli e applicarli, può costituire un deterrente per soggetti come amministrazioni locali che dispongono di risorse limitate. Questa difficoltà operativa è stata rilevata anche nello studio pubblicato sulla rivista Information[101], nel quale si sottolinea come la gestione di ecosistemi federati richieda non solo standard tecnici condivisi ma anche capacità di coordinamento tra attori diversi. Come osservato dai ricercatori «data governance requires coordination mechanisms among the actors participating in the data ecosystem», evidenziando come la complessità organizzativa della federazione possa rappresentare una delle principali sfide per l'adozione concreta del modello. In questo contesto, anche la gestione delle catene di fiducia, delle self-description e dei meccanismi di compliance multilivello può risultare onerosa per operatori non specialistici. Riprendendo l'intervista a Leonardo Lorenzetto, spesso la complessità tecnica delle specifiche e dei criteri di compliance richiede un supporto esterno o un livello di competenze interne che non tutte le organizzazioni possiedono.

Un altro limite importante viene evidenziato da alcuni critici riguardo all'apertura di GAIA-X, che pur essendo un valore in termini di competitività, comporta rischi di predominanza tecnica dei grandi attori già presenti. Riprendendo l'analisi di Antonio Cisternino, egli ritiene che la presenza di attori globali nell'ecosistema possa portare questi soggetti a influenzare la definizione degli standard per trarne vantaggio, piuttosto che una reale diversità di offerta. Ciò implica che è necessario bilanciare apertura e tutela degli interessi europei, stabilendo

[99] F. M. R. Livelli, *Analisi del TCO (total cost of ownership): differenze tra cloud sovrano e hyperscaler*, in Agenda Digitale, https://www.agendadigitale.eu/procurement/analisi-del-tco-total-cost-of-ownership-differenze-tra-cloud-sovrano-e-hyperscaler/, ultimo accesso marzo 2026.
[100] M. Scott, F. Bonfiglio, *Why Europe's Cloud Ambitions Have Failed, in Redirecting Europe's AI Industrial Policy*, AI Now Institute, https://ainowinstitute.org/publications/xi-why-europes-cloud-ambitions-have-failed, ultimo accesso marzo 2026.
[101] M. Zorrilla, J. Yebenes, *Architecture Building Blocks for Data Governance in Data Spaces, in Information*, https://www.mdpi.com/2078-2489/16/11/927, ultimo accesso marzo 2026.

una governance molto attenta e misure di mitigazione specifiche. Questa criticità è coerente anche con le letture date nel documento di Autolitano e Pawlowska, dove l'apertura dell'iniziativa viene interpretata come un possibile rischio di "cattura" da parte di attori extra-UE. Viene esplicitamente citato il dilemma del "Trojan Horse"[102], in cui la partecipazione di hyperscaler potrebbe lasciare invariata la direzione dei flussi di valore della data economy europea.

Inoltre, un ulteriore ostacolo riguarda la tempistica e l'adozione su larga scala. Anche se molte organizzazioni sono membri dell'associazione, l'adozione effettiva delle specifiche, dei federation services e dei criteri di compliance nelle implementazioni reali rimane in molti stati europei ancora in una fase iniziale. Una percezione simile emerge in una discussione organizzata dal Transatlantic AI Exchange[103] con rappresentanti di imprese e istituzioni partecipanti a GAIA-X, dove diversi imprenditori hanno sottolineato come l'iniziativa presenti ancora una distanza tra gli obiettivi dichiarati e le applicazioni concrete. Nel confronto è stato osservato che «there still seems to be a certain gap between the vision and the reality experienced by entrepreneurs», evidenziando come, nonostante il forte consenso sugli obiettivi, la trasformazione di tali principi in opportunità economiche e implementazioni operative proceda con maggiore lentezza rispetto alle aspettative iniziali. Per molte catene di valore industriali, la transizione verso modelli federati richiede investimenti in formazione, strumenti e adattamento dei processi IT, che non sempre coincidono con le priorità immediate di business. Questo porta a un ritmo di adozione che può risultare più lento di quanto previsto dai sostenitori iniziali del progetto. Come osservato dalla lettura sui data spaces[104], «cross-organizational coordination costs also represent an inherent obstacle in the development of data-sharing ecosystems», poiché richiedono l'allineamento di standard tecnici, modelli dati e processi organizzativi tra più partecipanti. Anche per questo motivo, dopo una fase iniziale di forte attenzione pubblica al progetto, soprattutto tra il 2019 e il 2022, il dibattito su GAIA-X ha conosciuto un rallentamento, mentre l'implementazione concreta delle iniziative procede con tempi più graduali.

---

[102] S. Autolitano, A. Pawlowska, *Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study,* IAI Papers 21|14, Istituto Affari Internazionali, 2021, p. 15-17.
[103]Transatlantic AI Exchange, *Gaia-X in the entrepreneur discussion: Great vision, when will reality come?*, https://transatlanticaiexchange.com/gaia-x-in-the-entrepreneur-discussion-great-vision-when-will-reality-come/, ultimo accesso marzo 2026.
[104] M. Zorrilla, J. Yebenes, *Architecture Building Blocks for Data Governance in Data Spaces, in Information*, https://www.mdpi.com/2078-2489/16/11/927, ultimo accesso marzo 2026.

Nonostante queste premesse, non deve essere sottovalutato che alcuni risultati si stanno già manifestando in progetti nell'ambito sanitario, di mobilità o manifatturiero, mostrando che la federazione può facilitare scambi sicuri e tracciabili di dati in contesti dove la fiducia e la compliance sono requisiti stringenti, contribuendo così al rafforzamento dell'economia digitale europea.[105]

Una valutazione più ampia e strutturata del progetto è stata proposta nel rapporto EuroStack[106], che delinea una strategia per la costruzione di un'intera filiera digitale europea. In questo documento gli autori inseriscono GAIA-X all'interno di un progetto europeo più grande per il raggiungimento della sovranità digitale, sottolineando come essa sia un passaggio fondamentale ma non sufficiente. Il framework può contribuire a definire regole e standard comuni, ma non è in grado di colmare il divario con i grandi attori globali. In questa prospettiva la sovranità digitale richiede anche politiche industriali, investimenti e coordinamento strategico più ampio, all'interno del quale GAIA-X si configura come uno dei tasselli, ma non come la soluzione definitiva.

L'efficacia di tale indirizzo strategico appare però strettamente legata al rapporto tra governance pubblica e iniziativa privata. Riprendendo l'intervista a Bonfiglio, egli rileva che uno dei limiti storici delle iniziative europee risieda proprio nella tendenza dei decisori politici a sostituirsi all'industria nella definizione delle modalità tecniche: «European politicians replaced industry in defining 'how' to do things instead of focusing on 'what' needs to be done»[107]. Secondo questa interpretazione, la pretesa delle istituzioni di stabilire gli standard tecnologici senza un reale allineamento con le dinamiche di mercato avrebbe paradossalmente reso più complessa la costruzione di alternative competitive rispetto ai grandi provider globali.

In sintesi, i risultati di GAIA-X vanno letti in una prospettiva di maturazione graduale del mercato, piuttosto che come una rivoluzione immediata. Ha già contribuito a strutturare un linguaggio comune, diffondere requisiti tecnici e creare spazi di cooperazione, ma deve

[105] Tardieu Hubert, *Role of Gaia-X in the European Data Space Ecosystem*, in ResearchGate, https://www.researchgate.net/publication/362180478_Role_of_Gaia-X_in_the_European_Data_Space_Ecosystem, ultimo accesso marzo 2026.
[106] F. Bria, P. Timmers, F. Gernone, *EuroStack – A European Alternative for Digital Sovereignty*, in Bertelsmann Stiftung, 2025.
[107] M. Scott, F. Bonfiglio, *Why Europe's Cloud Ambitions Have Failed, in Redirecting Europe's AI Industrial Policy*, AI Now Institute, https://ainowinstitute.org/publications/xi-why-europes-cloud-ambitions-have-failed, ultimo accesso marzo 2026.

ancora dimostrare la sua capacità di trasformare significativamente la struttura del mercato cloud europeo.

La valutazione complessiva dipende quindi dalla chiave di lettura adottata. Se interpretiamo l'ecosistema come un'infrastruttura immateriale di regole e fiducia, i traguardi raggiunti appaiono coerenti con la visione originale. Qualora, invece, l'aspettativa fosse quella di una risposta industriale immediata e competitiva verso gli attori privati, l'attuale distanza tra ambizioni e realizzazioni concrete mette in luce la complessità delle sfide strutturali e operative ancora aperte. In questa prospettiva, GAIA-X rappresenta il principale tentativo europeo di riequilibrio delle asimmetrie tra Stato e piattaforme attraverso l'architettura delle regole, collocandosi come progetto di ristrutturazione del quadro di governance del mercato cloud europeo.

Conclusioni

La presente tesi si è posta l'obiettivo di analizzare il rapporto tra stati, piattaforme digitali e controllo delle informazioni nell'economia contemporanea, ponendo l'attenzione su come il concetto di sovranità digitale viene tradotto in politiche pubbliche e soluzioni operative. Attraverso un percorso articolato su tre capitoli, è stata esaminata in un primo momento la trasformazione dell'ecosistema digitale e la centralità che le piattaforme digitali hanno ottenuto nella società contemporanea; successivamente l'analisi ha riguardato la strategia normativa e industriale sviluppata dall'Unione Europea per rafforzare il controllo sui dati; infine si è concentrata sul progetto GAIA-X, iniziativa che mira a costruire un sistema federato di servizi cloud e spazi di dati basato su principi di interoperabilità, trasparenza e fiducia.

L' obiettivo principale è stato valutare se iniziative di questo tipo possano contribuire a riequilibrare il rapporto di forza tra istituzioni pubbliche e piattaforme globali. In altri termini, l'analisi condotta permette di formulare alcune considerazioni su come l'Europa possa sviluppare strumenti capaci di ridurre la dipendenza tecnologica dai grandi attori privati e, al contempo, rafforzare il proprio controllo su infrastrutture e dati.

Il primo elemento emerso riguarda la trasformazione dell'ecosistema digitale. Le piattaforme, infatti, hanno progressivamente assunto il ruolo di infrastrutture fondamentali per l'economia contemporanea, offrendo servizi cloud, ambienti applicativi e strumenti di gestione dati su cui si basano la maggior parte delle attività economiche e amministrative. In questo contesto, sebbene i dati rappresentino una risorsa strategica, il loro valore effettivo dipende dalle infrastrutture preposte alla loro gestione. Per questo motivo, il controllo di tale asset diventa una leva di potere significativa, capace di influenzare non solo i mercati, ma anche le capacità di intervento degli stati.

Questa trasformazione ha implicazioni rilevanti anche sul piano politico e istituzionale. La crescente centralità dei sistemi virtuali mostra come il controllo delle tecnologie e delle piattaforme, attraverso cui i dati vengono gestiti, rappresenti oggi una dimensione cruciale dell'autonomia nazionale. In un contesto in cui gli attori privati dispongono di capacità tecnologiche e finanziarie superiori a quelle pubbliche, gli stati si trovano a dover affrontare nuovi e complessi limiti nella propria capacità di regolazione e intervento.

Per rispondere a queste dinamiche, l'Unione Europea ha sviluppato negli ultimi anni una strategia volta a rafforzare la propria autonomia strategica e la capacità di governare i flussi di dati, attraverso l'elaborazione dell'European Data Strategy e l'adozione di nuovi strumenti normativi. Tuttavia, come emerso nel corso dell'analisi, la sola dimensione giuridica non appare sufficiente a riequilibrare le attuali asimmetrie del mercato digitale. La sovranità digitale richiede infatti anche strumenti tecnici e modelli strutturali che permettano di tradurre tali principi legislativi in configurazioni operative concrete.

In questo contesto si inserisce il progetto GAIA-X, analizzato nel terzo capitolo come uno dei principali tentativi europei di costruire un ecosistema basato su standard condivisi e meccanismi di interoperabilità. Piuttosto che creare un nuovo provider europeo centralizzato, l'iniziativa propone un'architettura federata capace di rendere più trasparenti e confrontabili i servizi cloud, consentendo agli utenti di mantenere un maggiore controllo sulle proprie risorse informative e riducendo i fenomeni di vendor lock-in da singoli fornitori.

Allo stesso tempo, l'analisi ha evidenziato anche i limiti di questo approccio, che rendono difficile immaginare un riequilibrio immediato degli attuali assetti di mercato, quali la forte concentrazione del mercato cloud nelle mani di pochi hyperscaler, i costi di migrazione tra provider e la complessità tecnica dei sistemi federati. In questo senso, GAIA-X non può essere interpretato come una soluzione definitiva, quanto come un tentativo di ridefinire progressivamente le regole di funzionamento dell'ambiente digitale.

In questa prospettiva, alcune riflessioni emerse nel corso dell'analisi suggeriscono come il rafforzamento dell'autonomia digitale europea possa passare anche attraverso modelli più aperti. L'adozione di componenti open source e di standard tecnici accessibili a una pluralità di attori può contribuire a ridurre le dipendenze tecnologiche da singoli fornitori, favorendo maggiore trasparenza e verificabilità delle infrastrutture digitali. Infatti, a differenza dei modelli completamente proprietari, le tecnologie open source permettono maggiori possibilità di controllo e adattamento da parte di attori pubblici e privati. In questo senso, la disponibilità di componenti condivisi e di standard aperti può facilitare l'interoperabilità tra servizi e infrastrutture diverse, rendendo più semplice l'integrazione tra piattaforme e riducendo alcune dinamiche di dipendenza tecnologica. L'approccio federativo promosso da GAIA-X può quindi essere interpretato anche come un tentativo di combinare logiche di mercato, governance pubblica e modelli di innovazione aperta.

Nel complesso, l'analisi sviluppata in questa tesi mostra come la sovranità digitale rappresenti una questione complessa che non può essere affrontata attraverso un singolo strumento. Essa richiede un insieme coordinato di politiche pubbliche, capacità infrastrutturali e modelli di governance capaci di ridurre le dipendenze tecnologiche e di rafforzare la capacità delle istituzioni di governare l'ecosistema digitale. In questo quadro, iniziative come GAIA-X assumono un valore significativo non tanto per la creazione di nuove infrastrutture centralizzate, quanto per il tentativo di definire un insieme di regole, standard e principi condivisi che possano favorire la costruzione di un ecosistema digitale più interoperabile e trasparente.

In questa prospettiva, il dibattito sui dati deve rimanere centrale, soprattutto alla luce della crescente importanza dei dati nei processi economici e nelle dinamiche di innovazione tecnologica. La capacità dell'Europa di sviluppare modelli infrastrutturali e di governance capaci di coniugare apertura del mercato e controllo sui dati rappresenterà uno degli elementi chiave per la definizione degli equilibri futuri dell'economia digitale. In questo senso, progetti come GAIA-X possono essere interpretati come uno dei primi tentativi di costruire un modello europeo di organizzazione delle infrastrutture digitali, nel quale interoperabilità, trasparenza e collaborazione tra attori diversi diventino strumenti fondamentali per rafforzare l'autonomia tecnologica e la capacità di governo dell'ecosistema dei dati.

Bibliografia

Fonti primarie

Autolitano, S., Pawlowska, A. (2021). *Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study*. Istituto Affari Internazionali, IAI Papers 21|14.

Commissione Europea (2020). *Open Source Software Strategy 2020–2023*. Comunicazioni della Commissione europea, C (2020) 7149 final.

Commissione Europea (2020). *Una strategia Europea per i dati*. COM (2020) 66 final.

Federal Ministry for Economic Affairs and Energy (BMWi) (2020). *GAIA-X: Technical Architecture*. Berlin: BMWi.

Gaia-X European Association for Data and Cloud AISBL (2021). *Gaia-X Federation Services (GXFS).* Bruxelles: Gaia-X AISBL.

Gaia-X European Association for Data and Cloud AISBL (2022). *Gaia-X Architecture Document 22.04 Release*. Bruxelles: Gaia-X AISBL.

Gaia-X European Association for Data and Cloud AISBL (2022). *Gaia-X Policy Rules and Labelling Document Release 22.04.* Bruxelles: Gaia-X AISBL.

Gaia-X European Association for Data and Cloud AISBL (2022). *Gaia-X Trust Framework - 22.04 Release*. Bruxelles: Gaia-X AISBL.

Gaia-X European Association for Data and Cloud AISBL (2024). *Gaia-X Compliance Document*. Bruxelles: Gaia-X AISBL.

Gaia-X European Association for Data and Cloud AISBL (2025). *Market-X 2025 - Plenary Room*. Bruxelles: Gaia-X AISBL.

Gaia-X Hub Deutschland c/o acatech (2024). *Setting the course: Gaia-X and the future of data-centric government*. Gaia-X Hub Deutschland.

Madiega, T. (2020). *Digital sovereignty for Europe*. European Parliamentary Research Service (EPRS). Briefing Paper, PE 651.992.

Fonti secondarie

Berners-Lee, T. (1999). *Weaving The Web. The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*. New York: Harper Business.

Blotta, D. (2023). *Digitalizzazione dei sistemi di welfare, verso nuovi oligopoli? Il caso di Amazon Web Services*. Riviste Web.

Bria, F., Timmers, P., Gernone, F. (2025). *EuroStack – A European Alternative for Digital Sovereignty*. Bertelsmann Stiftung.

Commissione Europea (2021). *2030 Digital Compass: the European way for the Digital Decade*. COM (2021) 118 final.

Cuppini, N., Frapporti, M., Sandro, M., & Maurilio, P. (2022). *Il capitalismo nel tempo delle piattaforme. Infrastrutture digitali, nuovi spazi e soggettività algoritmiche*. Rivista Italiana di Filosofia Politica.

ENISA - European Union Agency for Cybersecurity (2025). *ENISA Threat Landscape 2025*. Bruxelles: ENISA.

Frapporti, M. (2023). *Il potere delle piattaforme come infrastrutture. Tecnica, estetica, egemonia*. Scienza & Politica.

Gineikyte-Kanclere, V., Eggert, M., Skiotyte, G. (2025). *European Software and Cyber Dependencies.* European Parliament Research Service, PE 780.413.

Hubert, T. (2022). *Role of Gaia-X in the European Data Space Ecosystem. https://www.researchgate.net/publication/362180478_Role_of_Gaia-X_in_the_European_Data_Space_Ecosystem*. Ultimo accesso: marzo 2026.

Lundell, B., Gamalielsson, J., Kats, A., Lindroth, M. (2023). *Avoiding lock-in effects through obtaining all necessary licences before use of a SaaS solution in a public sector organisation: a case study*. European Journal of Law and Technology, vol. 14, n. 1.

Parlamento Europeo, Consiglio dell'Unione Europea (2016). *Regolamento (UE) 2016/679 (GDPR)*. Gazzetta ufficiale dell'Unione Europea, L 119.

Parlamento Europeo, Consiglio dell'Unione Europea (2019). *Regolamento (UE) 2019/881 (Cybersecurity Act)*. Gazzetta ufficiale dell'Unione Europea, L 151.

Parlamento Europeo, Consiglio dell'Unione Europea (2022). *Direttiva (UE) 2022/2555 (NIS2).* Gazzetta ufficiale dell'Unione Europea, L 333.

Parlamento Europeo, Consiglio dell'Unione Europea (2022). *Regolamento (UE) 2022/868 (Data Governance Act).* Gazzetta ufficiale dell'Unione Europea, L 152.

Parlamento Europeo, Consiglio dell'Unione Europea (2023). *Regolamento (UE) 2023/2854 (Data Act).* Gazzetta ufficiale dell'Unione Europea, L 2023/2854.

Persson, P., Linåker, J. (2024). *Soft-lockins in Public Sector Acquisitions of Open Source Software-solutions: A Case Study on a Municipal E-Service Platform*. Cornell University, arXiv preprint.

Plantin, J.-C., Lagoze, C., Edwards, P., & Sandvig, C. (2016). *Infrastructure studies meet platform studies in the age of Google and Facebook.* New Media & Society.

Srnicek, N. (2017). *Capitalismo Digitale. Google, Facebook, Amazon e la nuova economia del web*. Roma: Luiss.

Zuboff, S. (2019*). Il capitalismo della sorveglianza*. Roma: Luiss University Press.

Sitografia

Fonti primarie

Cisternino, A. (2021). *Gaia-X, in crisi il cloud europeo? Le sfide da superare, con l'ingerenza delle big tech*. https://www.agendadigitale.eu/infrastrutture/gaia-x-anatomia-di-un-cloud-le-sfide-delleuropa-e-lingerenza-delle-big-tech/. Ultimo accesso: marzo 2026.

Dal Co, M. (2022). *Polo strategico per il cloud, un errore puntare su un 'campione nazionale': ecco perché*. https://www.agendadigitale.eu/infrastrutture/polo-strategico-per-il-cloud-un-errore-puntare-su-un-campione-nazionale-ecco-perche/. Ultimo accesso: marzo 2026.

Dipartimento per la trasformazione digitale (s.d.). *Strategia Cloud Italia - La strategia cloud per la Pubblica Amministrazione*. https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/stabile/4_la_strategia_cloud_per_la_pubblica_amministrazione.html. Ultimo accesso: febbraio 2026.

Gaia-X European Association for Data and Cloud AISBL (2025). *Gaia-X 2025 – Insieme verso un'infrastruttura dati federata e sicura*. https://gaia-x.eu/wp-content/uploads/2025/07/Gaia-X-Brochure_Overview_ITALIAN_ONLINE_012026.pdf. Ultimo accesso: febbraio 2026.

Polo Strategico Nazionale (s.d.). *Chi siamo*. https://www.polostrategiconazionale.it/chi-siamo/polo-strategico-nazionale/. Ultimo accesso: febbraio 2026.

Polo Strategico Nazionale (s.d.). *Public Cloud*. https://www.polostrategiconazionale.it/soluzioni/servizi-con-cloud-service-provider/public-cloud/. Ultimo accesso: febbraio 2026.

Polo Strategico Nazionale (s.d.). *Soluzioni*. https://www.polostrategiconazionale.it/soluzioni/. Ultimo accesso: febbraio 2026.

Scott, M., Bonfiglio, F. (2024). *Why Europe's Cloud Ambitions Have Failed, in Redirecting Europe's AI Industrial Policy*. https://ainowinstitute.org/publications/xi-why-europes-cloud-ambitions-have-failed. Ultimo accesso: marzo 2026.

Transatlantic AI Exchange (s.d). *Gaia-X in the entrepreneur discussion: Great vision, when will reality come?*. https://transatlanticaiexchange.com/gaia-x-in-the-entrepreneur-discussion-great-vision-when-will-reality-come/. Ultimo accesso: marzo 2026.

Zorrilla, M., Yebenes, J. (2025). *Architecture Building Blocks for Data Governance in Data Spaces.* https://www.mdpi.com/2078-2489/16/11/927. Ultimo accesso: marzo 2026.

Fonti secondarie

Aruba (2021). *Aruba favorisce lo sviluppo del cloud aperto e aderisce a GAIA-X*. https://www.aruba.it/magazine/cloud/aruba-favorisce-lo-sviluppo-del-cloud-aperto-e-aderisce-a-gaia-x.aspx. Ultimo accesso: marzo 2026.

Google. (2024). *AI, personalization, and the future of shopping*. https://blog.google/products/ads-commerce/ai-personalization-and-the-future-of-shopping/. Ultimo accesso: gennaio 2026.

Kumar, N. (2025). *Big Data Statistics 2026 (Growth, Trends & Market Size)*. https://www.demandsage.com/big-data-statistics/. Ultimo accesso: gennaio 2026.

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books.

Livelli, F. M. R. (2026). *Analisi del TCO (total cost of ownership): differenze tra cloud sovrano e hyperscaler*. https://www.agendadigitale.eu/procurement/analisi-del-tco-total-cost-of-ownership-differenze-tra-cloud-sovrano-e-hyperscaler/. Ultimo accesso: marzo 2026.

Marcellino, G. (2025). *Lock in del cloud, come tutelarsi: i consigli dei fornitori del servizio*. https://www.agendadigitale.eu/infrastrutture/lock-in-del-cloud-come-tutelarsi-i-consigli-dei-fornitori-del-servizio. Ultimo accesso: febbraio 2026

Martin, K., Armstrong, R. (2025). *Is the US stock market too concentrated?* https://www.ft.com/content/2652beb6-c6b8-488e-b189-c1ec926d584b. Ultimo accesso: gennaio 2026.

Richter, F. (2026). *AWS Stays Ahead as Cloud Market Accelerates*. https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/. Ultimo accesso: febbraio 2026.

Sinha, S. (2025). *State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally.* https://iot-analytics.com/number-connected-iot-devices. Ultimo accesso: gennaio 2026.

Solon, O. (2018). *Facebook says Cambridge Analytica may have gained 37m more users' data*. https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought. Ultimo accesso: gennaio 2026.

Strazi, G. (2019). *Il potere delle piattaforme digitali tra economia e politica.* https://eticaeconomia.it/il-potere-delle-piattaforme-digitali-tra-economia-e-politica/. Ultimo accesso: gennaio 2026.

Treccani (s.d.). *Creative Commons*. https://www.treccani.it/enciclopedia/creative-commons_(Lessico-del-XXI-Secolo)/. Ultimo accesso: marzo 2026.

Treccani (s.d.). *Sicurezza informatica*. https://www.treccani.it/enciclopedia/sicurezza-informatica/. Ultimo accesso: febbraio 2026.

Treccani (s.d.). *Sovranità.* https://www.treccani.it/enciclopedia/sovranita/. Ultimo accesso: gennaio 2026.

Appendice 1

Di seguito è riportata la trascrizione dell'intervista realizzata con Paolo Fontechiari, Responsabile della S.O. Infrastrutture Tecnologiche e Telecomunicazioni del Comune di Parma. L'intervista è stata condotta il 29 gennaio 2026 e si inserisce nell'analisi del rapporto tra istituzioni pubbliche e piattaforme digitali approfondita nel Capitolo 1.

Il comune di Parma ha intrapreso un percorso di digitalizzazione attraverso soluzioni cloud Lepida e It.City. Quali effetti ha avuto, nel tempo, sulla gestione delle infrastrutture e dei dati del comune?

Il percorso di trasformazione digitale del Comune di Parma, basato su due assi principali, i servizi cloud di Lepida e il contratto di servizio con It.City, ha prodotto negli anni una serie di effetti significativi sulla gestione delle infrastrutture tecnologiche e sulla governance dei dati dell'ente, che possono essere riassunti in:

- Esternalizzazione evoluta e razionalizzazione delle infrastrutture ICT.
  L'adozione dei servizi di data center Lepida in modalità in house providing ha permesso al Comune di razionalizzare e consolidare i sistemi ICT.
  Il Comune utilizza infrastrutture cloud Lepida come blade-as-a-service, storage e backup centralizzati, riducendo complessità, costi e frammentazione dei sistemi interni;
- Efficientamento della gestione delle reti, dei data center e delle telecomunicazioni.
  Il rapporto operativo con Lepida riguarda datacenter, rete in fibra, e servizi di telecomunicazione, consentendo una gestione più integrata e standardizzata delle infrastrutture;
- Contenimento dei costi operativi;
- Evoluzione nella governance dei dati;
- Miglioramento della sicurezza e delle misure di protezione;
  La Struttura Operativa ICT del Comune si occupa di cybersecurity, privacy e misure minime di sicurezza, integrate con gli standard Lepida e con la governance It.City;
- Consolidamento della gestione del dato territoriale;

La collaborazione con Lepida e Università di Parma ha portato allo sviluppo del Digital Twin della città, un ecosistema avanzato per la raccolta, condivisione e simulazione dei dati urbani;

- Impatti organizzativi e operativi;
- Miglioramento dei processi interni e dello smart working;

La scelta di affidarsi a fornitori cloud locali o in-house è motivata anche da esigenze di maggiore controllo e sovranità sui dati rispetto alle soluzioni offerte dai grandi provider globali (Microsoft, Google, AWS…)?

La scelta del Comune di Parma, e di molte pubbliche amministrazioni della Regione Emilia-Romagna, di utilizzare quando tecnicamente possibile fornitori cloud locali o in-house è fortemente motivata da esigenze di maggior controllo, conformità normativa e riduzione dei rischi legati ai grandi provider globali. Il tema centrale non è solo "dove risiedono i dati", ma chi controlla l'infrastruttura, e quali soggetti possono accedere ai dati. La PA, trattando dati sensibili o "importanti" è esposta anche ai rischi di dipendenza da grandi provider. La scelta di infrastrutture in-house come Lepida, secondo noi, consente maggiore autonomia operativa e migliore controllo, supportato da data center realizzati in Emilia-Romagna e in conformità ACN, ma anche la riduzione del rischio di vendor lock-in. Si tratta quindi di una scelta non solo tecnica ed economica, ma anche politica e strategica.

Nel medio-lungo periodo, le soluzioni cloud locali risultano più sostenibili rispetto ai grandi provider globali, oppure presentano criticità in termini di costi, aggiornamento tecnologico, servizi e flessibilità?

Il cloud locale garantisce al Comune di Parma un elevato livello di controllo, governance e compliance dei dati, risultando oggi una scelta sostenibile anche grazie alle condizioni favorevoli offerte dalle aziende in-house come Lepida e It.City. In uno scenario tecnologico sempre in evoluzione questo modello potrebbe mostrare limiti strutturali, soprattutto in termini di innovazione, scalabilità e capacità di tenere il passo con gli hyperscaler globali, molto più avanzati nello sviluppo di nuovi servizi e infrastrutture.

Quali criteri vengono utilizzati nella selezione dei fornitori cloud (ad esempio sicurezza, costi, affidabilità, conformità normativa) e quanto incidono eventuali vincoli normativi o linee guida nazionali nelle scelte dell'ente?

La selezione dei fornitori da parte del Comune di Parma non è mai stata una scelta libera o discrezionale, ma si colloca all'interno di un quadro normativo definito dall'Agenzia per la Cybersicurezza Nazionale (ACN), da AgID, dal Piano Triennale per l'Informatica nella PA e dal Codice degli Appalti, che stabiliscono requisiti obbligatori per sicurezza, conformità e qualità dei servizi cloud.

Fino all'avvio dei progetti PNRR, il modello adottato dall'ente ha privilegiato un'impostazione in-house, basata sull'utilizzo di servizi IaaS ("*Blade as a Service*") forniti da Lepida e dalle piattaforme software gestite da It.City.

Con il PNRR e l'evoluzione del mercato, sempre più orientato verso soluzioni SaaS, il Comune ha iniziato a integrare anche servizi cloud esterni. Tuttavia, questi vengono selezionati tra i fornitori che rispettano i criteri stabiliti a livello nazionale: sicurezza, affidabilità, interoperabilità, portabilità, sostenibilità economica e conformità normativa. In particolare, dal 1° agosto 2024, l'utilizzo di servizi cloud è consentito solo se qualificati da ACN, un requisito diventato imprescindibile per qualsiasi fornitore. A ciò si aggiunge la valutazione di costi complessivi e sostenibilità economica.

In che modo il Comune mantiene il controllo sui dati quando questi sono gestiti attraverso cloud di fornitori esterni?

Per cercare di garantire il controllo sui dati, adottiamo un insieme di misure che dovrebbero assicurano sicurezza, trasparenza e governance.

In particolare:

- Utilizzo esclusivo di fornitori qualificati ACN, condizione che assicura il rispetto dei requisiti minimi di sicurezza e conformità richiesti alla PA;
- Classificazione dei dati e, per alcuni servizi, la replica dei database su infrastrutture nei data center Lepida, oltre all'impiego di orchestratori per monitorare e gestire in modo centralizzato flussi, integrazioni e comportamenti applicativi;

- Adozione di standard in materia di sicurezza, portabilità, interoperabilità e tracciabilità;
- Contratti strutturati con SLA puntuali, nei quali vengono definiti tempi di risposta, responsabilità, livelli di servizio attesi e obblighi sul trattamento del dato;
- Attività di audit e monitoraggio continuo, condotte in collaborazione con It.City, che presidia il sistema informativo comunale e verifica costantemente la corretta gestione dei dati e l'aderenza ai requisiti normativi e tecnici.

Il tema della sovranità digitale è centrale nei processi decisionali legati all'adozione di piattaforme? In che forma?

Per il Comune di Parma, la "sovranità digitale" è centrale e prende forma concreta attraverso:

- Lepida per l'infrastruttura pubblica e la prossimità dei dati;
- It.City per la conduzione e la governance del sistema informativo;
- PSN + Regolamento ACN come perimetro per la selezione e la collocazione dei carichi, in funzione della classificazione dei dati.

L'affidamento a provider esterni introduce, secondo la vostra esperienza, forme di dipendenza tecnologica o contrattuale nel medio-lungo periodo?

Il rischio di dipendenza esiste (soprattutto con SaaS). Il Comune di Parma cerca di gestirlo con una serie di salvaguardie: infrastruttura pubblica Lepida, governance It.City, perimetro ACN/PSN, architetture orchestrate e interoperabili, repliche DB e clausole di uscita.

La Governance applicativa per noi centrale viene esercitata da It.City, che governa e conduce il sistema informativo comunale; ciò permette di standardizzare integrazioni, presidiare gli accessi, documentare i flussi e inserire controlli/audit regolari sui fornitori terzi, riducendo il rischio di dipendenza a livello applicativo/processo. It.City mantiene ownership di architetture, mapping dei dati, logiche di interoperabilità (es. orchestratori per flussi e API), così da evitare legami tecnici "a stella" direttamente con i fornitori esterni.

Le normative attuali sono sufficienti a garantire la sovranità dei dati e il controllo delle infrastrutture digitali, oppure ritiene necessari strumenti aggiuntivi?

Le normative attuali (Regolamento ACN, PSN, NIS2, DORA, Data Act, AI Act) hanno creato una base molto più solida e sicura rispetto al passato. Crediamo però che non siano ancora sufficienti, ad esempio non forniscono pieno controllo sulla catena tecnologica dell'AI, non risolvono completamente i problemi di portabilità e lock-in, non semplificano gli audit e la supervisione delle infrastrutture esterne.

Avete riscontrato delle criticità nell'utilizzo di infrastrutture cloud esterne? È nell'interesse del comune di valutare strategie o modelli alternativi per rafforzare l'autonomia infrastrutturale?

Personalmente credo che l'uso di cloud esterni possa introdurre dipendenze tecnologiche e contrattuali nel medio-lungo periodo, per contenerle si dovrebbe rafforzare modelli ibridi, pubblici e interoperabili, per migliorare autonomia infrastrutturale e di reversibilità tecnica.

Appendice 2

Di seguito è riportata la trascrizione dell'intervista realizzata con l'avvocato Francesco Montesi, consulente legale specializzato in privacy, protezione dei dati e diritto delle tecnologie digitali. L'intervista è stata condotta il 22 febbraio 2026 e si inserisce nell'analisi del quadro normativo europeo relativo alla governance dei dati e alla sovranità digitale, approfondito nel Capitolo 2.

Riguardo al tema della sovranità digitale, quali sono le principali normative europee in materia di dati? Queste affrontano esplicitamente il tema, oppure si concentrano prevalentemente su sicurezza, protezione e gestione del rischio?

Le principali normative europee in materia di dati che affrontano il tema della sovranità digitale sono il Regolamento generale sulla protezione dei dati (GDPR, Reg. (UE) 2016/679), il Data Act (Reg. UE 2023/2854), il Data Governance Act (DGA), il Digital Services Act (DSA), il Digital Markets Act (DMA), la direttiva Open Data (dir. 2019/1024/UE) e il Regolamento sulla libera circolazione dei dati non personali (Reg. (UE) 2018/1807). Queste normative non si limitano a sicurezza, protezione e gestione del rischio, ma affrontano esplicitamente anche il tema della sovranità digitale. La strategia europea per i dati, delineata dalla Commissione europea nella comunicazione del 19 febbraio 2020, mira a promuovere una "sovranità tecnologica europea" e a creare un mercato unico digitale, riducendo la dipendenza da soggetti extraeuropei e rafforzando il controllo europeo sui dati (Comunicazione Commissione europea 19.2.2020; Reg. (UE) 2016/679; Reg. (UE) 2018/1807).

Le norme attuali pongono vincoli reali sulla scelta dei fornitori cloud da parte delle pubbliche amministrazioni, oppure si limitano a regolare le modalità di utilizzo e di protezione dei dati?

Le norme attuali pongono vincoli reali sulla scelta dei fornitori cloud da parte delle pubbliche amministrazioni, andando oltre la semplice regolazione delle modalità di utilizzo e protezione dei dati. In particolare, il regolamento nazionale sul cloud per le PA prevede che i servizi cloud possano essere erogati solo da soggetti pubblici, società in house o società a

controllo pubblico (decreto legislativo 19 agosto 2016, n. 175), e impone un processo di qualificazione e verifica di conformità da parte dell'Agenzia Nazionale per la Cybersicurezza (ACN). Le amministrazioni devono trasmettere all'ACN l'elenco dei dati e servizi digitali, che vengono classificati e sottoposti a verifica di conformità, con aggiornamenti obbligatori almeno biennali. Solo i fornitori che rispettano i requisiti tecnici, di sicurezza e affidabilità previsti dal regolamento possono essere scelti dalle PA, e l'ACN può effettuare verifiche periodiche per assicurare il mantenimento dei requisiti (art. 5, regolamento cloud PA).

A livello europeo, il GDPR (Reg. (UE) 2016/679) impone alle PA di garantire che i dati personali siano trattati solo da fornitori che rispettano i principi di protezione dei dati (art. 5 GDPR) e che eventuali trasferimenti extra SEE siano valutati secondo le disposizioni del capitolo V del GDPR e l'art. 48. Inoltre, le PA devono valutare la legislazione del paese extra SEE del fornitore cloud per verificare eventuali rischi di accesso ai dati da parte di autorità straniere.

Il GDPR può essere considerato uno strumento utile per la sovranità dei dati?

Il GDPR (Reg. (UE) 2016/679) può essere considerato uno strumento utile per la sovranità dei dati, anche se la sua finalità principale è la protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati nell'Unione (art. 1 GDPR). Il regolamento attribuisce rilievo sia alla tutela della persona sia alla funzione sociale dei dati, prevedendo che la protezione dei dati personali non sia un valore assoluto, ma debba essere bilanciata con altri diritti fondamentali, come la libertà d'impresa (considerando 4 GDPR; art. 41 Cost.) e la funzione sociale (considerando 6 e 10 GDPR).

Il GDPR rafforza la sovranità dei dati in quanto consente agli Stati e all'Unione europea di mantenere il controllo sulle modalità di trattamento e circolazione dei dati personali, imponendo limiti e condizioni anche ai trasferimenti verso paesi terzi (capo V GDPR). Inoltre, il diritto alla portabilità dei dati (art. 20 GDPR) attribuisce agli interessati un maggiore controllo sui propri dati, favorendo l'autodeterminazione digitale e la possibilità di scegliere dove e come i dati siano trattati.

Il Regolamento ACN e il Polo Strategico Nazionale introducono obblighi di sicurezza e qualificazione dei fornitori, ma incidono realmente sulla sovranità infrastrutturale?

Il Regolamento ACN e il Polo Strategico Nazionale (PSN) introducono obblighi stringenti di sicurezza e qualificazione dei fornitori, incidendo concretamente sulla sovranità infrastrutturale italiana. In particolare, la normativa prevede che le pubbliche amministrazioni possano affidarsi solo a fornitori qualificati secondo criteri stabiliti dall'Agenzia per la Cybersicurezza Nazionale (ACN), con verifiche periodiche e requisiti tecnici, organizzativi e di affidabilità molto stringenti (art. 108, d.lgs. 36/2023; L. 90/2024). Il PSN, quale infrastruttura cloud nazionale, è stato concepito per garantire che i dati strategici e critici delle PA siano gestiti su infrastrutture localizzate e controllate in Italia o comunque in ambito UE/NATO, riducendo la dipendenza da fornitori extraeuropei e rafforzando la sovranità digitale e infrastrutturale del Paese (L. 90/2024). Il Decreto del Presidente del Consiglio dei ministri previsto dalla L. 90/2024 stabilirà criteri di premialità per l'uso di tecnologie di cybersicurezza italiane, UE o di Paesi alleati, rafforzando ulteriormente il controllo nazionale sulle infrastrutture critiche. Le Linee Guida ACN e la normativa correlata impongono inoltre alle PA l'obbligo di censire e monitorare fornitori, sistemi e flussi di dati, adottare piani di sicurezza, continuità operativa e disaster recovery, e garantire la conformità a standard minimi di cybersicurezza (Direttiva NIS 2, n. 2022/2555; Determinazione ACN su D.lgs. 138/2024). Questi obblighi non si limitano a raccomandazioni tecniche, ma costituiscono veri e propri requisiti organizzativi e infrastrutturali, la cui violazione può comportare sanzioni e la sospensione della qualificazione dei fornitori (deliberazione ANAC 28 settembre 2022 n. 441).

La direttiva NIS2 rafforza gli obblighi di cybersecurity per soggetti essenziali e importanti: dal punto di vista giuridico, questa normativa può essere considerata uno strumento di sovranità digitale o resta confinata a una logica di gestione del rischio?

La direttiva NIS2 (direttiva (UE) 2022/2555) rafforza in modo significativo gli obblighi di cybersecurity per soggetti essenziali e importanti, ma il suo impianto giuridico va oltre la mera gestione del rischio. Pur prevedendo un approccio integrato e olistico alla gestione dei rischi di cybersicurezza, la NIS2 mira anche a garantire la resilienza e la sicurezza delle

infrastrutture digitali strategiche dell'Unione, ampliando l'ambito soggettivo e settoriale rispetto alla precedente NIS1 (direttiva (UE) 2016/1148). L'inclusione di enti pubblici, PMI e nuovi settori strategici, nonché l'armonizzazione delle misure a livello europeo, rappresentano un passo verso la tutela degli interessi collettivi e la riduzione della dipendenza da soggetti extra-UE, elementi centrali della sovranità digitale (direttiva (UE) 2022/2555; orientamenti Commissione Europea 14 settembre 2023). La direttiva impone obblighi prescrittivi e responsabilità interne definite, con rendicontazione continua e obbligo di notifica degli incidenti, rafforzando la capacità degli Stati membri di esercitare un controllo effettivo sulle infrastrutture critiche e sui dati strategici (Determinazione ACN 14 aprile 2025). Inoltre, la NIS2 si integra con altre normative europee (come il DORA e la direttiva CER) in una logica di "security by design" e "by default", contribuendo a costruire un quadro normativo che rafforza la sovranità digitale europea attraverso la sicurezza e la resilienza delle infrastrutture (Regolamento (UE) 2022/2554; direttiva (UE) 2022/2555).

In sintesi, la NIS2 non si limita a una logica di gestione del rischio, ma rappresenta uno strumento giuridico fondamentale per la sovranità digitale, poiché consente agli Stati membri e all'UE di esercitare un controllo strategico sulle infrastrutture digitali e sui servizi essenziali, garantendo sicurezza, resilienza e autonomia rispetto a minacce e influenze esterne.

Il Data Act affronta esplicitamente il problema della portabilità dei dati e del lock-in tecnologico. Dal punto di vista giuridico, questi strumenti sono sufficienti a ridurre la dipendenza strutturale dai grandi provider cloud o presentano limiti applicativi rilevanti?

Il Data Act (Reg. UE 2023/2854) affronta esplicitamente il problema della portabilità dei dati e del lock-in tecnologico, introducendo obblighi per i fornitori di servizi cloud e edge computing volti a facilitare il passaggio dei clienti da un fornitore all'altro. In particolare, il Data Act prevede che i fornitori debbano garantire la portabilità dei dati in formato strutturato, di uso comune e leggibile da dispositivo automatico, la disponibilità di interfacce aperte e la compatibilità con specifiche di interoperabilità aperte o norme armonizzate (art. 30, Reg. UE 2023/2854). Viene inoltre imposto il principio di buona fede e cooperazione tra fornitori per assicurare la continuità del servizio e il trasferimento tempestivo dei dati (art. 27, Reg. UE 2023/2854).

Dal punto di vista giuridico, questi strumenti rappresentano un passo avanti significativo per ridurre la dipendenza strutturale dai grandi provider cloud, poiché mirano a eliminare barriere tecniche, contrattuali e organizzative che ostacolano la libera scelta del fornitore e la concorrenza (art. 26-33, Reg. UE 2023/2854). Tuttavia, permangono alcuni limiti applicativi: gli obblighi sono attenuati per servizi altamente personalizzati o non offerti su larga scala commerciale (art. 31, Reg. UE 2023/2854); inoltre, la reale efficacia delle misure dipenderà dall'adozione di standard tecnici comuni e dalla cooperazione effettiva tra operatori.

Lo schema di certificazione cloud EUCS può essere considerato uno strumento idoneo a ridurre la dipendenza tecnologica della Pubblica Amministrazione dai grandi provider globali, oppure agisce esclusivamente sul piano della compliance tecnica?

Lo schema di certificazione cloud EUCS (European Cybersecurity Certification Scheme for Cloud Services), previsto dal Regolamento (UE) 2019/881 (Cybersecurity Act), non si limita esclusivamente alla compliance tecnica, ma può essere considerato uno strumento idoneo a ridurre la dipendenza tecnologica della Pubblica Amministrazione dai grandi provider globali. La certificazione europea, infatti, mira a uniformare i requisiti di sicurezza per i servizi cloud in tutta l'Unione, superando la frammentazione normativa tra i diversi Stati membri e favorendo la competitività dei fornitori europei rispetto a quelli extra UE (Regolamento (UE) 2019/881; D.Lgs. n. 123/2022).

Il riconoscimento reciproco delle certificazioni tra Stati membri consente ai fornitori europei di accedere più facilmente al mercato della PA, riducendo la necessità di ricorrere a provider globali che spesso detengono certificazioni proprietarie non riconosciute a livello europeo. Inoltre, la certificazione EUCS, soprattutto ai livelli più elevati, richiede la dimostrazione di requisiti di sicurezza avanzati, la resistenza agli attacchi e la conformità a standard europei, elementi che rafforzano la sovranità digitale e infrastrutturale (art. 7 D.Lgs. n. 123/2022; art. 54 Regolamento (UE) 2019/881).

Le normative europee attuali riescono effettivamente a limitare l'impatto di legislazioni extra-UE (come il Cloud Act statunitense) sull'accesso ai dati trattati da fornitori cloud operanti in Europa?

Le normative europee attuali, in particolare il GDPR (Reg. (UE) 2016/679) e il Data Act (Reg. UE 2023/2854), hanno introdotto strumenti per limitare l'impatto di legislazioni extra-UE come il Cloud Act statunitense sull'accesso ai dati trattati da fornitori cloud operanti in Europa. Il GDPR disciplina rigorosamente i trasferimenti di dati personali verso Paesi terzi, imponendo che tali trasferimenti siano consentiti solo se il Paese destinatario garantisce un livello di protezione adeguato o se sono adottate garanzie appropriate (capo V, GDPR). Il Data Act, invece, interviene anche sui dati non personali, prevedendo all'art. 32 che i fornitori di servizi di trattamento dati debbano adottare ogni precauzione per impedire l'accesso governativo internazionale e di Paesi terzi ai dati detenuti nell'Unione, e vietando trasferimenti o accessi che creerebbero un conflitto con il diritto dell'Unione o degli Stati membri. Solo in presenza di accordi internazionali specifici e di garanzie procedurali (motivazione, proporzionalità, controllo giurisdizionale) può essere consentito l'accesso ai dati da parte di autorità extra-UE (art. 32, Reg. UE 2023/2854). Tuttavia, la disciplina europea non elimina completamente il rischio di accessi extraterritoriali, soprattutto in assenza di accordi internazionali vincolanti e di un controllo effettivo sulle infrastrutture fisiche e giuridiche dei fornitori cloud. Il quadro normativo europeo rappresenta una risposta articolata e coerente per limitare l'impatto di normative come il Cloud Act, ma la sua efficacia pratica dipende anche dalla capacità di enforcement e dalla cooperazione internazionale (Data Act, art. 32; GDPR, capo V).

Appendice 3

Di seguito è riportata la trascrizione dell'intervista realizzata con Leonardo Lorenzetto, Presale Engineer & Solution Architect di SIR.tel. Srl, azienda operante nel settore delle infrastrutture ICT, della sicurezza e delle soluzioni cloud per la Pubblica Amministrazione e le imprese. L'intervista è stata condotta dall'autore il 27 febbraio 2026 e si inserisce nell'analisi tecnica e operativa del progetto GAIA-X e delle sue implicazioni nel mercato delle infrastrutture cloud, approfondita nel Capitolo 3.

Dal suo punto di vista tecnico e progettuale, come valuta oggi il progetto GAIA-X? Lo considera una reale infrastruttura alternativa o principalmente un framework di regole e standard?

Dal punto di vista tecnico, GAIA-X non si configura attualmente come un'infrastruttura alternativa in senso stretto, ossia come un cloud europeo dotato di proprie risorse fisiche o di una capacità computazionale autonoma rispetto ai provider esistenti.

Nella pratica operativa, i progetti che sviluppiamo per la Pubblica Amministrazione o per aziende regolamentate continuano a poggiare su infrastrutture già presenti sul mercato, siano esse hyperscaler o operatori nazionali qualificati.

In fase progettuale, quindi, GAIA-X incide più a livello di architettura logica e documentazione tecnica che a livello di infrastruttura fisica. Potrebbe influenzare il modo in cui definiamo le API, come strutturiamo le policy di accesso, come garantiamo la portabilità tra ambienti. Ma non cambia il fatto che, operativamente, i servizi cloud oggi sono ancora erogati dai grandi provider o da operatori nazionali già attivi.

Nella sua esperienza con la Pubblica Amministrazione, ha mai riscontrato una domanda di soluzioni conformi a logiche simili a quelle di GAIA-X (es. sovranità dei dati, controllo della localizzazione, interoperabilità)?

Negli ultimi anni si osserva con chiarezza una crescente attenzione verso requisiti che sono pienamente coerenti con la filosofia del progetto.

In particolare, nei capitolati tecnici più recenti – ad esempio nelle gare Consip di nuova generazione (Cloud v3) – emergono elementi molto significativi:

- valutazione dell'impatto normativo del fornitore rispetto alla gestione di infrastrutture critiche,
- attenzione alla territorialità dell'infrastruttura e alla giurisdizione applicabile,
- richiesta di qualificazioni ACN e utilizzo di cloud certificati o PSN,
- requisiti espliciti di interoperabilità e portabilità,
- percorsi di certificazione dei prodotti e servizi in relazione a criteri di sovranità digitale.

Per la prima volta nei capitolati tecnici ci sono riferimenti alla territorialità e alla sovranità che rappresentano un passaggio rilevante, la localizzazione e la giurisdizione diventano criteri di valutazione strutturati, non semplici dichiarazioni di conformità.

Si può quindi affermare che la domanda di sovranità digitale esiste, ma è formulata in termini normativi e regolatori più che come adesione a un marchio o a un ecosistema specifico. La PA richiede sovranità operativa e giuridica, chiede garanzie sulla gestione del dato e sulla catena di responsabilità. Se in futuro il framework venisse esplicitamente integrato nei criteri di gara o nei requisiti di qualificazione, il suo impatto sul mercato potrebbe diventare molto più diretto e sistemico.

Dal punto di vista tecnico, quanto è realmente possibile garantire sovranità dei dati in un ecosistema cloud federato?

La sovranità dei dati, intesa come completa autonomia tecnologica e industriale, è un obiettivo complesso da raggiungere in un contesto globale fortemente interconnesso. Questo perché anche quando i dati risiedono fisicamente in Europa o in Italia, l'hardware può essere prodotto in altri continenti, il firmware sviluppato da vendor globali e molte componenti software sono il risultato di ecosistemi internazionali.

Dal punto di vista tecnico-operativo, ciò che è concretamente garantibile oggi è una sovranità giuridica e operativa. Questo significa poter definire con precisione:

- la localizzazione fisica del dato,

- la giurisdizione applicabile,
- i soggetti autorizzati all'accesso,
- i meccanismi di audit e tracciabilità,
- le policy di utilizzo e condivisione effettivamente enforceable.

Parallelamente, si osserva un investimento crescente in infrastrutture locali. Diversi hyperscaler, tra cui Microsoft e altri operatori globali, stanno sviluppando data center in Italia, presentandoli come elementi di sovranità digitale nazionale e come hub strategici anche verso mercati limitrofi, inclusi alcuni Paesi africani. Questo dimostra che per competere realmente sul piano della sovranità digitale è necessario disporre di una base fisica adeguata sul territorio.

Tuttavia, per parlare di sovranità in senso industriale sarebbe necessario un ecosistema completo che includa produzione hardware, sviluppo software strategico e capacità di innovazione autonoma.

In questo quadro, GAIA-X può contribuire a strutturare le regole del gioco e a rafforzare il controllo e la trasparenza, ma non può, da solo, colmare il divario industriale e tecnologico rispetto ai grandi attori globali.

GAIA-X promette interoperabilità e riduzione del vendor lock-in. Nella pratica progettuale, quanto è realistico migrare servizi tra provider mantenendo piena portabilità applicativa e dei dati?

La questione del lock-in va distinta su più livelli.

A livello infrastrutturale (IaaS), oggi le architetture sono in larga parte standardizzate e questo rende tecnicamente possibile ricreare un'infrastruttura equivalente presso un altro provider.

Un nuovo operatore, se ha interesse commerciale ad acquisire il cliente, è generalmente in grado di replicare un'architettura simile in tempi ragionevoli. Da questo punto di vista, il lock-in puramente tecnico si è ridotto rispetto al passato.

Il tema si sposta quindi su due aspetti principali:

1. Il costo effettivo del servizio.
   Le infrastrutture cloud con livelli più elevati di performance, resilienza e servizi gestiti hanno inevitabilmente costi superiori. Spesso la scelta del provider è legata al bilanciamento tra qualità e costo. Migrare verso un'infrastruttura equivalente può comportare un aumento dei costi, oppure una riduzione delle funzionalità.
2. Le policy contrattuali e di migrazione.
   Le condizioni di uscita, la disponibilità dei dati in formato aperto, i tempi e i costi di recesso incidono in modo determinante. Alcuni operatori, inclusi provider italiani come Netalia, pongono esplicitamente l'assenza di lock-in contrattuale come elemento competitivo, offrendo canoni d'uso senza vincoli rigidi e politiche di migrazione trasparenti.

A livello PaaS e SaaS, invece, il lock-in assume una dimensione più complessa. Quando si adottano piattaforme applicative la dipendenza non è solo infrastrutturale ma organizzativa e procedurale. In questi casi, la migrazione implica la revisione dei processi interni, la formazione del personale e la riconfigurazione delle integrazioni.

Iniziative come GAIA-X possono contribuire ad aumentare la trasparenza e a favorire la portabilità infrastrutturale, ma la riduzione del lock-in applicativo dipende soprattutto dalle scelte architetturali e contrattuali adottate in fase di progetto.

L'adozione di standard di self-description, certificazioni multilivello e trust framework federati comporta un aumento di complessità tecnica. Secondo lei, il mercato della PA è pronto a sostenerne i costi e l'impatto organizzativo?

Le grandi amministrazioni centrali o i ministeri dispongono generalmente di strutture ICT interne e di governance più mature. Diverso è il caso delle amministrazioni locali o di enti di dimensioni ridotte. In molte realtà territoriali, le competenze tecniche sono limitate o fortemente esternalizzate. Spesso le funzioni di controllo, ad esempio DPO o referenti per la protezione dei dati, non dispongono di competenze tecniche approfondite sulle architetture cloud e sui modelli di servizio. Nella pratica, può risultare complesso da parte nostra far

distinguere con precisione tra IaaS, PaaS, SaaS o far comprendere pienamente l'impatto infrastrutturale di determinate scelte.
Se la complessità cresce eccessivamente, il rischio è che l'ente si affidi completamente al consulente o al fornitore stesso per interpretare le regole. In assenza di un rafforzamento delle competenze interne o di linee guida molto chiare, l'adozione di framework sofisticati potrebbe rimanere concentrata sui progetti più strategici o obbligatori.

Ritiene che iniziative come il Polo Strategico Nazionale o le qualificazioni ACN vadano nella stessa direzione di GAIA-X o rappresentino un modello diverso di sovranità digitale?

Queste iniziative si collocano certamente nella stessa traiettoria culturale e politica di GAIA-X, ossia nel rafforzamento della sovranità digitale e nella riduzione dei rischi legati alla gestione delle infrastrutture critiche. Tuttavia, operano su piani differenti.

Mentre GAIA-X è un modello distribuito, che punta a creare un ecosistema regolato ma non centralizzato, il PSN è uno strumento operativo, con infrastrutture fisiche dedicate e un perimetro di sicurezza ben definito.

Un elemento ancora in evoluzione riguarda il perimetro cibernetico nazionale. In origine, il PSN doveva inserirsi in modo più chiaro all'interno di questo perimetro, ma nel tempo si è osservato un rafforzamento dell'approccio di sicurezza anche in ambiti con maggiore rilevanza strategica, inclusi settori sensibili. Questo ha contribuito a rendere il modello più orientato alla chiusura e al controllo nazionale rispetto alla logica federata europea.

Per quanto riguarda i comuni e le amministrazioni locali, permane una certa incertezza operativa: non sempre è pienamente chiaro quali obblighi ricadano all'interno del perimetro nazionale e quali margini di autonomia siano consentiti nella scelta dei fornitori. Questo genera una fase di transizione in cui gli enti si orientano prevalentemente attraverso le qualificazioni ACN e le linee guida centrali.

Dal punto di vista di un system integrator, GAIA-X rappresenta un'opportunità concreta di business (nuovi servizi, certificazioni, consulenza), oppure un quadro ancora troppo teorico per generare domanda reale?

GAIA-X è ancora principalmente un'iniziativa in evoluzione. Non rappresenta, allo stato attuale, un driver diretto di domanda commerciale paragonabile, ad esempio, alle qualificazioni ACN o ai requisiti PSN, che incidono immediatamente sulle gare pubbliche.

Tuttavia, l'iniziativa può avere un impatto indiretto significativo. Se i principi e i meccanismi di GAIA-X verranno progressivamente integrati nei criteri di procurement o nelle normative europee, potrebbero generare nuove esigenze di consulenza, adeguamento architetturale e certificazione.

Per un system integrator è comunque utile monitorare l'evoluzione del framework, perché potrebbe incidere sulle future qualificazioni e sugli standard richiesti nei bandi

Considerando che GAIA-X non impone obblighi giuridici e si fonda su un'adesione volontaria, pensa che possa realmente modificare gli equilibri di mercato dominati dagli hyperscaler, oppure rischia di rimanere uno standard di conformità adottato solo in contesti specifici?

l principale punto di forza di GAIA-X è aver trasformato il concetto di sovranità digitale da tema prevalentemente politico o teorico in una struttura tecnica concreta, fondata su standard, ontologie, meccanismi di certificazione e strumenti di verifica.

Il limite strutturale, tuttavia, riguarda la dimensione industriale e infrastrutturale. La mancanza di una piena sovranità tecnologica europea comporta che molte grandi istituzioni, soprattutto in ambiti critici, si trovino a dover bilanciare esigenze di sicurezza, compliance e accesso a tecnologie avanzate che spesso sono sviluppate da operatori globali.

In alcuni casi, l'assenza di un ecosistema europeo completamente autonomo può rendere più complessa l'adozione di soluzioni cloud in contesti particolarmente sensibili. Parallelamente, dal lato degli utenti finali – sia pubblici che privati – la domanda di servizi cloud è in crescita costante, soprattutto in modalità ibrida.

Molte organizzazioni stanno valutando modelli infrastrutturali ibridi per conciliare esigenze di controllo locale con flessibilità e scalabilità del cloud pubblico. In queste valutazioni pesa molto anche il costo dell'hardware e dell'infrastruttura on-premise: l'investimento iniziale e

i costi di gestione possono risultare significativi, spingendo verso soluzioni cloud o ibride più efficienti sotto il profilo economico.

La natura volontaria di GAIA-X può certamente rappresentare un limite sotto il profilo dell'impatto sistemico. Un framework non vincolante dipende dalla sua capacità di generare valore percepito e vantaggio competitivo per gli operatori che decidono di aderirvi.

In generale credo che GAIA-X può contribuire a definire regole comuni e aumentare la trasparenza, ma da solo non è sufficiente a colmare il divario industriale né a sostituire la necessità di investimenti infrastrutturali concreti. Il suo impatto dipenderà dalla capacità di integrarsi stabilmente nelle politiche industriali e nei meccanismi di procurement europei.

Ringraziamenti

Oggi si conclude un importante capitolo della mia vita. Desidero quindi ringraziare tutte le persone speciali che mi hanno accompagnato durante questo percorso.

Un sentito ringraziamento va al Professor Mattia Frapporti, per la guida attenta, la competenza e l'attenzione con cui ha seguito la stesura di questa tesi. Il suo supporto ha reso possibile il completamento di questo lavoro con serenità.

Ai miei genitori devo tutto ciò che sono oggi. Grazie per gli insegnamenti e per il sostegno che non mi avete mai fatto mancare. Grazie per aver creduto in me, per avermi spinto oltre i limiti e per avermi dato ogni giorno la forza di sognare in grande. Grazie per avermi concesso la libertà di sbagliare e di sperimentare, facendomi capire che l'errore non è un fallimento, ma parte del percorso. I vostri sacrifici, la vostra dedizione e il vostro affetto mi hanno permesso di essere la persona che sono oggi.

Un pensiero speciale va alla mia famiglia, ai nonni e agli zii, per il supporto e l'affetto che non mi hanno mai fatto mancare. La vostra vicinanza è sempre stata un sostegno silenzioso ma fondamentale, capace di offrirmi una parola di incoraggiamento o un momento di meritata spensieratezza. Grazie per aver partecipato a ogni mio traguardo e per essere parte integrante del mio percorso.

Desidero poi ringraziare gli amici di sempre, anche a chi, dopo anni, non ha ancora del tutto chiaro in cosa mi sono laureato. Grazie per aver condiviso con me ogni momento, dalle occasioni più semplici -tisana e lamentele-, ai viaggi fatti insieme, tra scleri, risate e biscotti sottomarca. Grazie per avermi ascoltato, supportato e soprattutto sopportato. Siete stati il mio sostegno, la spinta necessaria nei momenti di incertezza, le persone a cui raccontavo le soddisfazioni più grandi e le difficoltà che sembravano insormontabili. La vostra compagnia ha reso questo percorso non solo più leggero, ma profondamente speciale. Se è vero che gli amici te li scegli, beh, io posso dire di aver scelto proprio bene!

Un grazie speciale va ai miei compagni di uni. È merito di questa amicizia, nata per caso tra i banchi, se le ore interminabili a lezione sono volate. Tra un caffè dal Romano, un salto alla Pam, gli aperitivi post esame e le serate finite a fare festa, siamo diventati amici per davvero e in modo del tutto inaspettato. Grazie perché senza di voi questi tre anni non sarebbero stati

la stessa cosa, da ognuno ho imparato qualcosa di unico, che porterò via con me insieme a questa laurea.

Un ringraziamento immenso va a SF6. Grazie per aver saputo trasformare un semplice appartamento in qualcosa che potessi chiamare casa, e dei semplici coinquilini nella mia famiglia a Bologna. Anche se non è mai stata la casa più bella, pulita e profumata che tanto speravo, è stata sicuramente il luogo dove mi sentivo al sicuro, dove rifugiarsi dopo una brutta giornata e dove poter parlare di tutto. Dai momenti più semplici come le birrette sul balcone o a quelli più pazzi come le feste del 25 aprile, avete reso la mia esperienza universitaria un'avventura che non dimenticherò mai. Grazie per aver condiviso con me il caos, le nostre storie e la quotidianità di questi anni.

Un pensiero va anche a Lemonade, o, come la chiamano i miei amici, "la setta". Se è vero che «viviamo per le notti che nessuno ricorda, con persone che non dimenticheremo mai», allora al centro di tutto questo ci sono proprio tutti gli incontri fatti: sconosciuti con cui ho condiviso tanto, e che si sono trasformati in compagni di viaggio indimenticabili. In questo stracasino ho trovato persone splendide che hanno saputo darmi tanto, ben oltre semplici slogan. Grazie per le esperienze fatte, le serate, le trasferte e per avermi insegnato che il sonno è una cosa di cui sappiamo gran poco.

E infine grazie Bologna, perché sei stata il luogo dove tutto questo è potuto accadere. Grazie per la tua pazzia, la tua allegria, i tuoi portici infiniti, le persone che mi hai fatto conoscere e le esperienze che mi hai fatto vivere. Mi hai accolto e mi hai cambiato, lasciandomi molto più di una semplice laurea. Mi piace molto la teoria secondo la quale non ci innamoriamo di una città, ma della persona che lì si sente possibile: per me quella città sei tu.

Il ringraziamento finale va a me stesso, perché bravi tutti, ma quello che si è laureato qui sono io. Grazie perché non ho sottovalutato la mia forza e ho dato valore ai miei sacrifici, allo sforzo nascosto e alle nottate in bianco. Grazie per averci creduto sempre, per la pazienza e per la determinazione che mi hanno portato fino a questo traguardo. E infine grazie al me bambino: spero di averti reso orgoglioso dell'adulto che siamo diventati.

Grazie a tutti!