Sovereignty-washing dei Big Tech: come gli hyperscaler vendono Sovranità Digitale senza garantirla



Il **sovereignty-washing** dei Big Tech è la nuova frontiera del marketing ingannevole nell'ecosistema cloud europeo. Dietro white paper patinati, keynote rassicuranti e impegni contrattuali dal linguaggio studiato, i principali hyperscaler statunitensi – Microsoft, Amazon Web Services e Google Cloud – stanno vendendo ai governi e alle imprese del Vecchio Continente un'idea di *sovranità digitale* che, quando messa alla prova dei fatti, si rivela strutturalmente vuota.

Il termine ricalca dinamiche già note in altri settori: così come il *greenwashing* traveste pratiche ambientali superficiali da impegni ecologici autentici, il sovereignty-washing confeziona soluzioni cloud "sovrane" che, nella sostanza, non modificano il rapporto di dipendenza giurisdizionale tra il cliente europeo e il fornitore statunitense. La differenza, in questo caso, è che la posta in gioco non riguarda l'immagine aziendale, ma la sicurezza nazionale, la protezione dei dati sensibili dei cittadini e l'autonomia strategica di un intero continente.

Per i professionisti della sicurezza informatica – CISO, SOC analyst, security architect, esperti di compliance – comprendere i meccanismi del sovereignty-washing non è un esercizio accademico. È una necessità operativa. Perché ogni decisione di procurement cloud che ignora la distinzione tra *data residency* e *data sovereignty* espone l'organizzazione a rischi giuridici, geopolitici e di continuità operativa che nessun Service Level Agreement può mitigare.

Sovereignty-washing: definizione e anatomia di una strategia

Che cos’è il sovereignty-washing

Il sovereignty-washing descrive la pratica con cui i fornitori cloud commercializzano soluzioni di *data residency* – ovvero la localizzazione geografica dei server – come se fossero soluzioni di *data sovereignty* autentica, cioè il pieno controllo giurisdizionale e operativo sui dati.

Nella sua forma più comune, il sovereignty-washing si manifesta attraverso un repertorio prevedibile: apertura di data center sul territorio europeo, assunzione di personale locale, creazione di entità giuridiche sussidiarie nell’UE, partnership con operatori nazionali e, soprattutto, un’intensa attività comunicativa che utilizza il lessico della sovranità – “controllo locale”, “residenza dei dati”, “trasparenza”, “indipendenza operativa” – per descrivere architetture che restano, nella loro struttura profonda, soggette alla giurisdizione statunitense.

Come ha osservato l’economista della concorrenza Cristina Caffarra, tra le promotrici dell’iniziativa EuroStack, il sovereignty-washing rappresenta una versione più sofisticata della stessa tattica che ha già neutralizzato Gaia-X: cooptare il linguaggio dell’autonomia per consolidare la dipendenza.

La distinzione cruciale: residenza vs. sovranità dei dati

Per i professionisti della sicurezza, la distinzione tecnico-giuridica tra questi due concetti è il punto di partenza per qualsiasi valutazione:

- **Data residency**: indica *dove* i dati sono fisicamente

archiviati. È una questione geografica. Risponde alla domanda: “In quale Paese si trovano i server?”
- **Data sovereignty**: è un principio più ampio, legato al *controllo giurisdizionale*. Risponde alla domanda: “Le leggi di chi governano questi dati? Chi può accedervi e a quali condizioni?”

Per anni si è assunto che la residenza determinasse la sovranità: se i dati erano in Germania, la legge tedesca ed europea si applicava. Questa assunzione è stata demolita dalla portata extraterritoriale di legislazioni come il CLOUD Act statunitense e il FISA Section 702. La localizzazione fisica dei server non garantisce più la protezione giurisdizionale.

Il CLOUD Act: l’elefante nella stanza

Il **CLOUD Act** (Clarifying Lawful Overseas Use of Data Act), approvato nel 2018, obbliga le aziende tecnologiche statunitensi a fornire dati alle autorità USA su richiesta legale, *indipendentemente* dal luogo fisico in cui tali dati sono conservati. Questo significa che un server Microsoft a Francoforte, un bucket S3 di AWS a Milano o un’istanza Google Cloud a Parigi sono tutti potenzialmente accessibili dal governo americano.

L’articolo 48 del GDPR stabilisce che i trasferimenti di dati verso autorità di Paesi terzi richiedono una base giuridica, come un trattato di mutua assistenza giudiziaria (MLAT). Il CLOUD Act, tuttavia, aggira esplicitamente il meccanismo MLAT, creando un conflitto giuridico strutturale e irrisolto tra diritto europeo e diritto statunitense.

Quando le promesse crollano: i fatti del 2025

La testimonianza sotto giuramento al Senato francese

Il momento più emblematico del fallimento narrativo del sovereignty-washing si è consumato il 10 giugno 2025, nelle aule del Senato francese. Anton Carniaux, direttore degli affari pubblici e legali di Microsoft France, interrogato sotto giuramento nell'ambito di un'indagine sugli appalti pubblici e la sovranità digitale, ha risposto alla domanda se potesse garantire che i dati dei cittadini francesi non sarebbero mai stati trasmessi alle autorità USA senza il consenso delle autorità francesi.

La risposta è stata inequivocabile: *non posso garantirlo*. Carniaux ha confermato che, in presenza di una richiesta giuridicamente valida da parte del governo americano, Microsoft sarebbe obbligata a ottemperare – anche se ciò configura una violazione del GDPR e della legislazione francese.

Nelle settimane successive, dichiarazioni analoghe sono emerse da rappresentanti di AWS, Google e Salesforce, tutti i quali hanno ammesso che consegnerebbero dati di clienti europei alle autorità statunitensi se obbligati da un ordine giudiziario. Kevin Miller, VP dei data center globali di AWS, ha dichiarato esplicitamente di non poter garantire che i dati di una PMI tedesca non vengano divulgati alle autorità americane.

Queste ammissioni hanno fatto crollare in poche settimane una narrazione costruita con investimenti miliardari in marketing e relazioni istituzionali. Come ha sintetizzato Frank Karlitschek, CEO di Nextcloud: ciò che i Big Tech dichiarano in un'aula di tribunale rivela molto più di quanto dicano in un comunicato stampa.

Il caso ICC-Microsoft: il kill switch non è più ipotetico

A febbraio 2025, l'amministrazione Trump ha imposto sanzioni alla Corte Penale Internazionale (ICC) dell'Aja, in risposta ai mandati di arresto emessi nei confronti del primo ministro israeliano Benjamin Netanyahu. La conseguenza diretta e immediata è stata la disconnessione dell'account di posta Outlook del Procuratore Capo Karim Khan, che si è trovato impossibilitato ad accedere alle comunicazioni ufficiali dell'istituzione.

Microsoft ha successivamente contestato la ricostruzione, sostenendo di non aver "sospeso i servizi" all'ICC. Tuttavia, il danno – tanto operativo quanto reputazionale – era già compiuto. Il Procuratore Khan è stato costretto a migrare su Proton Mail, servizio svizzero con crittografia end-to-end. Entro ottobre 2025, l'ICC ha annunciato la migrazione completa dei propri sistemi verso openDesk, una piattaforma open source sviluppata nell'ambito dell'iniziativa tedesca per la sovranità digitale.

Il caso ICC ha trasformato il concetto di "digital kill switch" – il rischio che un governo straniero possa, attraverso le proprie aziende tecnologiche, interrompere servizi digitali critici di organizzazioni o Stati – da scenario teorico a precedente documentato. Per qualsiasi CISO di un'istituzione europea, la lezione è brutale: un SLA non protegge dalla geopolitica.

L'ecosistema del sovereignty-washing: tattiche e architetture

Le "sovereign cloud" degli hyperscaler:

un’analisi critica

Nel corso del 2025, tutti e tre gli hyperscaler principali hanno rilanciato le proprie offerte “sovrane” per il mercato europeo:

- **Microsoft** ha presentato gli “European Digital Sovereignty Commitments”, rinominando i precedenti “European Cloud Principles”, con promesse di elaborazione dati in-country per Microsoft 365 Copilot in 15 Paesi e l’espansione di Azure Local
- **Google** ha introdotto il servizio “Cloud Air-Gapped”, con tenancy completamente isolata per clienti con requisiti normativi stringenti
- **AWS** ha annunciato la creazione di un’unità cloud con sede nell’UE, nel tentativo di creare una separazione giurisdizionale

Ciascuna di queste offerte presenta miglioramenti tecnici reali: crittografia gestita dal cliente, personale residente nell’UE, separazione logica e fisica delle infrastrutture. Tuttavia, nessuna di esse risolve il problema fondamentale: il *control plane* – il livello di gestione e orchestrazione dell’infrastruttura cloud – resta sotto il controllo della società madre statunitense. E con esso, resta l’esposizione alla giurisdizione americana.

Come ha osservato il VMware Cloud Foundation Blog in un’analisi dettagliata: la vera domanda non è *dove* si trovano i dati, ma *chi* li controlla.

Il modello partnership-con-operatore-locale: il caso Bleu

Un’architettura particolarmente insidiosa di sovereignty-washing è quella che interpone un operatore locale tra l’hyperscaler e il cliente. Il caso emblematico è Bleu, la joint venture tra Orange, Capgemini e Microsoft per offrire

servizi cloud “sovrani” alla pubblica amministrazione francese.

Il modello promette che un’entità giuridica francese operi il data center, utilizzando la tecnologia Microsoft sotto licenza. Tuttavia, la dipendenza tecnologica permane: aggiornamenti software, patch di sicurezza, funzionalità del control plane e, in ultima analisi, la continuità del servizio dipendono dalla collaborazione attiva di Microsoft. Il senatore Simon Uzenat, presidente della commissione d’inchiesta, ha sottolineato la contraddizione: l’istituzione promette sovranità, ma la catena del valore rimane ancorata a un fornitore extraeuropeo.

Il precedente Gaia-X: lezioni non apprese

L’iniziativa Gaia-X, lanciata nel 2019 come progetto franco-tedesco per un ecosistema cloud federato europeo, rappresenta il precedente più istruttivo. L’intenzione originaria era valida: creare un framework di interoperabilità e fiducia per i cloud provider europei. Il problema, come ha ricostruito Cristina Caffarra, è stato che Microsoft, Google e AWS hanno ottenuto di essere inclusi nel consorzio. Una volta dentro, l’iniziativa ha perso la propria ragion d’essere, producendo principalmente standard e specifiche tecniche senza impatto commerciale reale.

Il rapporto Draghi sulla competitività del 2024 ha sostanzialmente certificato il fallimento di Gaia-X nel modificare il panorama competitivo del mercato cloud europeo. Le quote di mercato dei provider europei sono scese dal 27% del 2017 al 15% attuale, mentre i tre hyperscaler statunitensi controllano quasi i due terzi dell’intero mercato cloud continentale.

Il quadro normativo europeo: strumenti contro il sovereignty-washing

Il Cloud Sovereignty Framework della Commissione Europea

A ottobre 2025, la Commissione Europea ha pubblicato il **Cloud Sovereignty Framework** (CSF), un sistema di criteri per valutare e classificare il livello di sovranità dei servizi cloud negli appalti pubblici dell'UE. Il framework definisce otto obiettivi di sovranità:

- **Sovranità strategica**: radicamento nel tessuto giuridico, finanziario e industriale dell'UE
- **Sovranità legale e giurisdizionale**: protezione da ingerenze giuridiche extraeuropee
- **Sovranità operativa**: controllo effettivo sulle operazioni da parte del cliente
- **Trasparenza della supply chain**: visibilità completa sulla catena di fornitura
- **Apertura tecnologica**: interoperabilità e assenza di lock-in proprietario
- **Sicurezza e compliance**: allineamento a NIS2, DORA, GDPR
- **Sostenibilità ambientale**
- **Resilienza e continuità operativa**

Il framework introduce i **Sovereignty Effectiveness Assurance Level** (SEAL) come soglia minima per la partecipazione ai bandi e un **Sovereignty Score** (SOV) per la valutazione competitiva. La prima applicazione concreta è stata il bando da 180 milioni di euro per servizi cloud sovrani, pubblicato contestualmente.

L'EUCS e l'impasse sui requisiti di

sovranità

Lo schema di certificazione EUCS (European Cybersecurity Certification Scheme for Cloud Services), sviluppato dall'ENISA ai sensi del Cybersecurity Act, avrebbe dovuto armonizzare i requisiti di sicurezza cloud a livello europeo. Tuttavia, il dibattito sulla possibilità di includere requisiti di *sovranità* – come l'obbligo di sede legale nell'UE per i livelli di assurance più elevati – ha paralizzato il processo decisionale.

I requisiti di sovranità erano presenti nelle bozze iniziali del 2023, poi rimossi nel 2024 sotto la pressione diplomatica e industriale statunitense. Diversi Stati membri, in particolare Francia e Italia, ne chiedono il ripristino. La revisione del Cybersecurity Act, prevista per la fine del 2025, potrebbe rappresentare l'occasione per superare lo stallo, introducendo "fattori di rischio non tecnici" nei framework di certificazione.

NIS2, DORA e Data Act: la rete normativa si stringe

Il quadro regolamentare europeo offre già strumenti significativi:

- La **Direttiva NIS2**, in vigore dal 2024, impone obblighi stringenti di gestione del rischio ICT e incident reporting anche ai fornitori di servizi cloud, con implicazioni dirette sulla valutazione dei rischi legati alla giurisdizione
- Il **Regolamento DORA** (Digital Operational Resilience Act), applicabile dal gennaio 2025, obbliga le istituzioni finanziarie a valutare i rischi geopolitici ed economici della propria catena di fornitura ICT, inclusa la lunghezza delle supply chain quando fornitori di Paesi terzi supportano funzioni critiche

- Il **Data Act**, in applicazione dal 12 settembre 2025, rafforza i diritti di portabilità e switching tra provider cloud, riducendo il lock-in contrattuale e tecnico che perpetua le dipendenze

La Dichiarazione per la Sovranità Digitale Europea, adottata dagli Stati membri il 18 novembre 2025, pur non essendo vincolante, sancisce formalmente l'ambizione di rafforzare la sovranità digitale come pilastro della resilienza economica e della sicurezza.

L'alternativa europea: tra EuroStack e migrazioni concrete

L'iniziativa EuroStack: dal manifesto all'azione

EuroStack è un'iniziativa industriale lanciata a settembre 2024 che riunisce oltre 200 organizzazioni – da PMI innovative a gruppi come Airbus – con l'obiettivo di costruire un ecosistema digitale europeo integrato, dalla connettività al cloud, dall'IA ai chip.

La proposta si articola su tre pilastri:

- **Buy European**: riformare le regole di procurement pubblico per dare priorità ai provider europei nelle infrastrutture critiche, come accade già in USA e Asia
- **Build European**: investimento del settore privato nello sviluppo di alternative europee, senza dipendere esclusivamente da sussidi pubblici
- **Fund European**: un veicolo finanziario dedicato, potenzialmente alimentato dal Digital Europe Programme o dalle sanzioni DMA/DSA, per sostenere lo sviluppo dello stack tecnologico europeo

I numeri della dipendenza sono allarmanti: l'80% della spesa

cloud e software delle istituzioni europee va a fornitori statunitensi. Il 99% dello stack cloud della Commissione Europea stessa gira su infrastrutture non europee, con la sola OVHCloud a rappresentare l'1% "sovrano".

Le migrazioni in corso: segnali dal campo

Nonostante la complessità della sfida, alcune migrazioni concrete sono in corso e offrono modelli replicabili:

- **Schleswig-Holstein (Germania)**: il Land ha cancellato circa il 70% delle licenze Microsoft, sostituendole con alternative open source, con l'obiettivo di utilizzare servizi Big Tech solo in casi eccezionali entro la fine del decennio
- **ICC (L'Aja)**: migrazione completa da Microsoft Office a openDesk, piattaforma open source sviluppata nell'ambito dell'iniziativa tedesca per la sovranità digitale
- **Francia – Progetto NUBO**: cloud privato basato su OpenStack sviluppato dal Ministero dell'Economia e delle Finanze per la gestione di dati sensibili
- **Consorzio EDIC Digital Commons**: istituito nel luglio 2025 da Germania, Francia, Italia e Paesi Bassi per sviluppare e scalare strumenti digitali sovrani

Queste esperienze dimostrano che, sebbene una rottura completa con gli hyperscaler USA sia irrealistica nel breve termine, migrazioni mirate per applicazioni ad alto rischio sono possibili e già in corso.

Sovereignty-washing e cybersecurity: le implicazioni operative

Per il CISO: valutare il rischio giurisdizionale

Il sovereignty-washing introduce una classe di rischio che i framework tradizionali di risk management spesso sottovalutano: il **rischio giurisdizionale**. Questo rischio non è mitigabile con controlli tecnici convenzionali (crittografia, segmentazione, access control), perché opera a un livello superiore – quello del potere legale di uno Stato estero di forzare l'accesso ai dati, indipendentemente dalle protezioni implementate.

Per un CISO, le implicazioni operative includono:

- **Revisione delle valutazioni di rischio**: integrare il rischio giurisdizionale nelle analisi di impatto per tutti i servizi cloud erogati da provider soggetti a legislazione extraeuropea
- **Due diligence sulla supply chain**: verificare non solo il provider diretto, ma l'intera catena di controllo, incluso il control plane, i sistemi di billing e il supporto tecnico
- **Pianificazione di exit strategy**: sviluppare piani di migrazione verso alternative europee o multi-cloud per i workload più sensibili
- **Clausole contrattuali rafforzate**: richiedere trasparenza su tutti gli accessi ai dati, inclusi quelli derivanti da richieste governative, con meccanismi di notifica al cliente

Checklist anti-sovereignty-washing per security architect

Un security architect chiamato a valutare un'offerta "sovereign cloud" dovrebbe porsi le seguenti domande:

- **Controllo**: chi opera la piattaforma e ha accesso al

control plane?
- **Indipendenza giuridica**: il provider è interamente governato dal diritto UE, o esistono società madri extraeuropee?
- **Standard aperti**: è possibile migrare i workload verso un altro provider senza riscrivere tutto?
- **Trasparenza**: lo stack software è open source o verificabile, oppure vincolato ad API proprietarie?
- **Crittografia**: le chiavi di cifratura sono gestite dal cliente in modo crittograficamente indipendente dal provider?
- **Aggiornamenti**: il provider può cessare unilateralmente gli aggiornamenti o le patch di sicurezza?

Se la risposta alla maggior parte di queste domande è negativa, l'offerta presenta caratteristiche di sovereignty-washing.

Il rischio del "digital kill switch" nella gestione della continuità operativa

Il caso ICC ha reso tangibile uno scenario che, fino a pochi mesi prima, veniva liquidato come ipotesi estrema: un fornitore tecnologico che, in ottemperanza a sanzioni governative, disconnette unilateralmente un cliente dai servizi essenziali.

Per i responsabili della continuità operativa, questo scenario richiede un aggiornamento dei Business Impact Assessment (BIA) e dei Business Continuity Plan (BCP) che includa:

- La possibilità di interruzione improvvisa di servizi cloud per motivi geopolitici
- L'identificazione dei servizi critici per i quali non esistono alternative pronte all'uso
- Test periodici di migrazione d'emergenza verso provider alternativi
- Valutazione della resilienza degli strumenti di

comunicazione interna in caso di disconnessione forzata

Prospettive: verso una sovranità digitale autentica

Il Cloud and AI Development Act (CAIDA)

La Commissione Europea sta preparando il **Cloud and AI Development Act** (CAIDA), che dovrebbe introdurre un quadro regolamentare più strutturato per la politica cloud del settore pubblico. L'iniziativa si inserisce nel più ampio **AI Continent Action Plan** e potrebbe rendere operativi i principi del Cloud Sovereignty Framework, trasformandoli da strumenti di procurement volontari a requisiti vincolanti.

La revisione del Cybersecurity Act

La revisione del Cybersecurity Act, prevista per il 2026, rappresenta l'occasione decisiva per integrare i requisiti di sovranità nel framework di certificazione EUCS. L'introduzione di "fattori di rischio non tecnici" – una formula che riconosce che la sicurezza dei dati non può essere ridotta a misure puramente tecniche – potrebbe costringere gli Stati membri a esplicitare le considerazioni politiche alla base delle proprie posizioni.

Il rischio del sovereignty-washing nel Global South

Come ha evidenziato un'analisi pubblicata da Lawfare, le conseguenze del sovereignty-washing non si limitano all'Europa. Le stesse soluzioni "sovrane" confezionate per il mercato europeo vengono riproposte ai Paesi del Global South, dove la capacità di scrutinio tecnico e giuridico è spesso inferiore. La centralizzazione della risoluzione DNS nelle mani di pochi grandi attori, l'estensione dei servizi "air-

gapped” a contesti di regolamentazione debole e la standardizzazione di pratiche di data governance progettate per compiacere un regolatore europeo anziché proteggere realmente la sovranità locale sono tutti vettori di preoccupazione.

Conclusioni – Oltre il sovereignty-washing: decidere di costruire

Il sovereignty-washing dei Big Tech non è un difetto del sistema: è una caratteristica. È la risposta razionale di aziende che operano sotto la giurisdizione statunitense a una domanda di mercato che non possono soddisfare autenticamente. Nessuna architettura tecnica, per quanto sofisticata, può annullare il vincolo giuridico del CLOUD Act. Nessun contratto può prevalere su un ordine esecutivo del presidente degli Stati Uniti.

La domanda reale per l’Europa – e per ogni professionista della sicurezza che opera al suo interno – non è se gli hyperscaler stiano praticando sovereignty-washing. Lo stanno facendo, lo hanno ammesso sotto giuramento, e le evidenze empiriche lo confermano quotidianamente.

La domanda reale è: l’Europa ha la volontà collettiva di passare dalla denuncia alla costruzione? Di investire non solo in regolamenti e framework – dove eccelle – ma in infrastrutture, competenze e mercati – dove accusa un ritardo strutturale?

L’alternativa, come ha sintetizzato il report EuroStack, è chiara: un continente ridotto a colonia digitale, con industrie svuotate, cittadini sotto sorveglianza straniera e obiettivi climatici in ostaggio di monopoli.

Per i CISO, i security architect e i compliance officer europei, il sovereignty-washing non è un tema di policy

lontano. È un **rischio operativo presente**, da valutare, mitigare e – dove possibile – eliminare. Iniziando, oggi, dalla domanda più semplice e più scomoda: chi controlla davvero i dati che ci sono stati affidati?

Fonti principali:

Nextcloud Blog – Big Tech's "Sovereign Cloud" Promises Just Collapsed (ottobre 2025)

The Register – Europe Gets Serious About Cutting Digital Umbilical Cord (dicembre 2025)

Lawfare – Tech's Sovereignty Washing in Europe Will Ripple in the Global South (ottobre 2025)

The Register – Microsoft Exec Admits It Cannot Guarantee Data Sovereignty (luglio 2025)

VMware Cloud Foundation Blog – The Great Cloud Charade: Why Data Residency Isn't Data Sovereignty (novembre 2025)

Commissione Europea – Cloud Sovereignty Framework v1.2.1 (ottobre 2025)

Atlantic Council – Digital Sovereignty: Europe's Declaration of Independence? (gennaio 2026)

ECFR – Get Over Your X: A European Plan to Escape American Technology (dicembre 2025)

Grohmann, R. e Costa Barbosa, A. – Sovereignty-as-a-Service, Media, Culture & Society (2025)

EU ISS – Technical Is Political: When a Cloud Certification Scheme Divides Europe (novembre 2025)

Eurojust – The CLOUD Act

Commissione Europea – Data Act (in applicazione dal settembre 2025)

TechPolicy.Press – Europe Tried to Take Control of Its Digital Stack in 2025 (dicembre 2025)

CMS Law-Now – Demystifying the Debate on the US CLOUD Act vs European Data Sovereignty (febbraio 2026)

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/sovereignty-washing/