La transizione delle agenzie governative di tutto il mondo verso la sovranità digitale

Una nuova strategia di sopravvivenza per il settore pubblico

Per le organizzazioni pubbliche al di fuori degli Stati Uniti, la sovranità digitale ha assunto un significato che va ben oltre il semplice requisito normativo, diventando una vera e propria strategia di sopravvivenza. Le pubbliche amministrazioni sanno che garantire la sovranità e il rispetto delle leggi locali non è più sufficiente. Oggi infatti il nuovo obiettivo della sovranità digitale è l'autonomia strategica, ovvero la capacità di utilizzare, innovare e aggiornare i servizi critici in modo indipendente, anche se il supporto esterno dovesse essere sospeso o le catene di distribuzione globali interrotte.

Secondo un recente report della Conferenza delle Nazioni Unite sul Commercio e lo Sviluppo (UNCTAD), "il 79% dei Paesi che hanno leggi in materia di privacy e protezione dei dati è preoccupato per la sovranità digitale."[1] I governi non possono più permettersi di ignorare le dipendenze insite nei sistemi proprietari chiusi. Questo desiderio di ottenere l'autonomia strategica è influenzato da tre fattori chiave:

- **Rischio geopolitico:** In tempi normali affidarsi ad hyperscaler globali può essere una scelta sostenibile, ma in periodi di tensioni geopolitiche dipendere dal supporto esterno rappresenta una vulnerabilità critica. Infatti, la distruzione delle infrastrutture fisiche o le interruzioni della connessione Internet potrebbero paralizzare le operazioni basate sul cloud. È quindi essenziale che le nazioni siano in grado di agire in maniera autonoma quando la cooperazione internazionale risulta impossibile o inaffidabile. Per fare ciò occorrono sistemi in grado di operare in ambienti in cui la connettività di rete è assente, limitata o inaffidabile (DDIL) in modo che le funzioni essenziali per la missione, dai sistemi di comando e controllo della difesa ai servizi di emergenza per i cittadini, rimangano operative anche se il Paese è disconnesso dalla rete Internet globale.
- **Resilienza informatica:** Gli attacchi informatici commissionati da stati esteri ai danni di altre nazioni sono sempre più sofisticati, frequenti ed efficaci. La sovranità è fondamentale per assicurare la resilienza delle infrastrutture critiche, ad esempio le reti energetiche, i sistemi sanitari e le reti dei sistemi di difesa, contro le interferenze esterne e il sabotaggio della catena di distribuzione con cui gli utenti malintenzionati potrebbero trafugare dati sensibili ma anche inserire codice dannoso negli aggiornamenti software in transito. Condizione imprescindibile per le agenzie governative è quindi la capacità di verificare in maniera indipendente l'integrità della catena di distribuzione del software per prevenire il rischio di spionaggio esterno e garantire l'integrità dei sistemi.
- **Competitività economica:** Sempre più Paesi danno centralità alla sovranità digitale facendone un caposaldo della sicurezza nazionale. Intanto, localizzare lo sviluppo dell'IA e la governance dei dati permette agli stati di mantenere i motori della crescita economica futura sotto la loro giurisdizione interna, invece di lasciarli al controllo di terze parti. Crescono inoltre le preoccupazioni legate all'utilizzo di modelli di IA a scatola nera stranieri, che si teme potrebbero causare una perdita di proprietà intellettuale e rilevanza culturale. L'autonomia strategica consente alle nazioni di promuovere ecosistemi di innovazione locali e assicurare che il valore economico generato dalla loro trasformazione digitale rimanga all'interno dell'economia nazionale.

1 "Data protection and privacy legislation worldwide", UNCTAD, 17 febbraio 2026.

Un unico obiettivo, più realtà regionali

Per quanto gli stati abbiano tutti un unico obiettivo, ovvero migliorare il controllo, le influenze e gli ostacoli specifici che le pubbliche amministrazioni si trovano ad affrontare variano significativamente da regione a regione.

Europa, Medio Oriente, Africa (EMEA) e Canada

La sfida principale nella area EMEA è legata al bisogno di disporre di tecnologie avanzate e alla dipendenza da provider esterni all'Unione Europea (UE) che questo comporta. Questa dipendenza espone i governi a rischi giurisdizionali, pensiamo ad esempio alle leggi extraterritoriali emanate dagli Stati Uniti come il Clarifying Lawful Overseas Use of Data Act (CLOUD) o il precedente Foreign Intelligence Surveillance Act (FISA) del 1978.

Le agenzie governative europee sono soggette a una complessa rete di normative rigorose, tra cui il NIS2 dedicato alla sicurezza informatica e il Regolamento sulla resilienza operativa digitale (DORA), oltre alle normative nazionali come la certificazione SecNumCloud nel caso della Francia. L'infrastruttura di difesa europea risulta frammentata, anche a causa delle lacune nell'interoperabilità della NATO che ritardano lo scambio di dati. Si risconta inoltre una grave carenza di personale autorizzato a operare in ambienti sovrani. Sebbene geograficamente distante dall'area EMEA, il Canada condivide le medesime sfide, in particolare per quanto riguarda l'utilizzo di infrastrutture obsolete. Il Dipartimento della Difesa nazionale canadese si trova infatti alle prese con un'infrastruttura CSNI (Consolidated Secret Network Infrastructure) molto disorganica e ostacoli burocratici che rallentano l'adozione di funzionalità moderne. Quindi, per limitare i rischi e le esposizioni le agenzie governative della regione EMEA e del Canada si concentrano oggi principalmente sulla protezione dei dati sensibili dalle interferenze legali straniere e lavorano alla modernizzazione dei software puntando sullo sviluppo interno di nuove funzionalità.

Asia Pacifico (APAC)

Nella regione APAC le politiche sono caratterizzate da forti misure protezionistiche e da una rigorosa conformità normativa, finalizzate al raggiungimento dell'indipendenza tecnologica.

- **Localizzazione dei dati:** Paesi come la Cina, l'India e l'Indonesia applicano una rigorosa localizzazione dei dati, imponendo che i dati critici risiedano interamente all'interno dei confini nazionali e limitando l'uso dei cloud pubblici globali.
- **Elevata responsabilità:** Singapore impone rigorosi standard di sicurezza end to end, in base ai quali i funzionari pubblici possono incorrere in sanzioni penali in caso dovessero utilizzare in modo improprio o smarrire i dati, il che promuove una cultura di approvvigionamento molto conservativa.
- **Requisiti locali e globali:** Nella regione si prediligono i modelli glocal, ovvero partnership in cui la tecnologia globale viene erogata tramite aziende locali per garantire il controllo sovrano.

I Paesi dell'APAC si concentrano oggi principalmente sullo sviluppo di funzionalità native al fine di ridurre la dipendenza a lungo termine dalle potenze straniere e considerano la sovranità digitale come uno scudo contro la vulnerabilità geopolitica.

America Latina (LATAM)

Nella regione LATAM la modernizzazione è legata al concetto di continuità operativa ed è spesso ostacolata dall'instabilità strutturale piuttosto che dalle politiche.

- **Instabilità e discontinuità:** In un clima geopolitico incerto, i frequenti cambiamenti nella leadership politica e la volatilità economica compromettono la pianificazione IT a lungo termine e i contratti di approvvigionamento pluriennali.
- **Attenzione alla sicurezza interna:** Le agenzie di difesa della regione LATAM danno priorità alla sicurezza interna (protezione delle frontiere, lotta al narcotraffico) e privilegiano strumenti di sorveglianza agili anziché infrastrutture strategiche complesse.[2]

2 "New Pentagon strategy to focus on homeland, Western Hemisphere", DefenseNews, 25 settembre 2025.

- **Rischi dell'approvvigionamento:** Le inefficienze e i rischi di corruzione negli appalti pubblici riducono il valore effettivo dei budget tecnologici, rendendo necessario lo sviluppo di sistemi economici, aperti e flessibili, in grado di resistere ai tagli di bilancio e ai cambiamenti politici senza vincolare il Paese a fornitori proprietari costosi e poco elastici.

L'approccio di Red Hat alla sovranità digitale

Per raggiungere il loro obiettivo, le istituzioni pubbliche di tutto il mondo dovrebbero considerare la sovranità digitale in tutte le sue molteplici sfaccettature. E qui entra in gioco Red Hat che mette a disposizione gli strumenti e l'ecosistema giusti.

Sovranità dei dati e IA

Red Hat sa bene quanto è importante nel settore pubblico ottenere l'autonomia e il controllo completi dei dati critici e dei modelli di IA al fine di garantire la residenza dei dati entro i confini nazionali e allineare la governance alle normative locali. Le organizzazioni pubbliche devono implementare strategie di IA sovrana che permettano loro di mantenere sempre la proprietà dei modelli e dei dati per l'addestramento. Questo è possibile distribuendo i modelli e i dati su un'infrastruttura localizzata, anziché lavorare su modelli controllati da terze parti. Red Hat® OpenShift® AI consente il deployment di funzionalità di IA sovrana ovunque si trovino i dati. La piattaforma permette di monitorare la posizione e gli accessi ai dati utilizzando tecniche di elaborazione confidenziale per proteggere i dati in uso e garantisce la conformità a normative come il Regolamento sull'intelligenza artificiale dell'UE (AI Act).

Sovranità tecnologica

La capacità di eseguire i carichi di lavoro senza legarsi all'infrastruttura o ai software proprietari di uno specifico provider è un aspetto chiave per assicurarsi l'indipendenza a lungo termine e la possibilità di trasferire le applicazioni senza vincoli. Le amministrazioni pubbliche dovrebbero evitare il vendor lock-in prediligendo standard open source e piattaforme containerizzate. In questo modo se un provider dovesse modificare le sue policy o dovessero aumentare le tensioni geopolitiche, loro potranno trasferire agevolmente i carichi di lavoro su un'altra infrastruttura senza bisogno di eseguire il refactoring. Red Hat implementa standard open source e aiuta così i suoi clienti a ridurre il rischio di vendor lock-in. La nostra piattaforma supporta più architetture hardware (x86, Advanced RISC Machine (ARM), RISC-V). In questo modo i sistemi nazionali possono evolversi e aggiornarsi secondo i propri tempi e non sono vincolati da dipendenze esterne.

Sovranità operativa

Per sopravvivere e operare anche in condizioni di scarsa connettività, le agenzie governative devono mantenere la piena autorità amministrativa e garantire l'indipendenza delle operazioni IT critiche. La difesa e le infrastrutture principali devono quindi dare massima priorità alla resilienza operativa. Questo significa automatizzare i piani di ripristino di emergenza tenendo conto dei periodi di guerra e assicurarsi che il supporto e le operazioni siano gestiti da cittadini locali e autorizzati. Red Hat offre un servizio di assistenza sovrano. Questo servizio prevede che il supporto tecnico venga fornito da cittadini verificati (ad esempio cittadini dell'UE) e garantisce quindi che i dati a cui ha accesso il personale di supporto rimarranno all'interno di una specifica giurisdizione. Inoltre, mette a disposizione Red Hat Ansible® Automation Platform, una piattaforma ideale per automatizzare la resilienza poiché consente ripristino e applicazione di patch rapidi anche in ambienti disconnessi (DDIL).

Sovranità della sicurezza

La possibilità di verificare in maniera indipendente l'integrità, la sicurezza e l'affidabilità dei sistemi e dei processi digitali aiuta le agenzie a garantire la conformità. Le istituzioni devono passare dalla fiducia cieca ad una fiducia verificabile. Per fare ciò occorrono un controllo rigoroso della catena di distribuzione del software e la capacità di dimostrare la conformità a standard come Common Criteria, Federal Information Processing Standards (FIPS) e NIS2. Red Hat garantisce una catena di distribuzione del software affidabile che assicura software con firma crittografica, provenienza

verificata e una distinta base (SBOM). In questo modo le agenzie possono sempre controllare ogni componente e assicurarsi che non sia stato inserito codice dannoso. Queste misure di sicurezza aiutano a garantire che le agenzie rispettino i nuovo obblighi normativi, come il Regolamento sulla ciberresilienza (CRA) dell'UE.

Autonomia strategica grazie all'open source

Red Hat mette a disposizione una base flessibile e open source con cui le agenzie governative possono beneficiare di maggiore scelta e controllo e unificare le tecnologie isolate. Consapevole che un unico provider difficilmente avrà i mezzi per risolvere da solo il problema della sovranità digitale, Red Hat offre la possibilità di creare un cloud sovrano integrando le soluzioni cloud e infrastrutturali di diversi provider, evitando così i limiti di una singola soluzione.

Da oltre 30 anni Red Hat sviluppa soluzioni open source di livello enterprise affidabili e allineate ai più severi requisiti di sicurezza e conformità. L'open source enterprise non è una semplice tecnologia, ma è la base architetturale essenziale per consentire agli enti governativi di raggiungere l'autentica sovranità digitale e autonomia strategica. A differenza dei fornitori proprietari che si affidano a sistemi chiusi e poco trasparenti e richiedono fiducia cieca, Red Hat aiuta le organizzazioni a mantenere il controllo assoluto sul proprio futuro digitale. Un approccio open source può aiutare gli enti pubblici di tutto il mondo a controllare la velocità dell'innovazione globale, dall'edge tattico della rete all'IA sovrana, e garantire al contempo la portabilità e la resilienza dei carichi di lavoro. Può contribuire inoltre a proteggere le operazioni di importanza critica dai rischi del vendor lock-in e dell'obsolescenza tecnologica. I principi e le tecnologie open source promosse da Red Hat sono in linea con la nuova dottrina orientata alla scelta di soluzioni open source ("default to open") che sta trovando larga diffusione in zone come l'Unione Europea. L'utilizzo di un modello come questo scongiura il rischio di vendor lock-in e consente di ispezionare e modificare il codice, un aspetto essenziale per garantire la fiducia e la sicurezza nazionale.

- **Fiducia e trasparenza**

  Il modello open source di Red Hat offre la totale trasparenza. Gli enti governativi possono infatti ispezionare il codice sorgente, verificarne la sicurezza e controllare le catene di distribuzione del software. Questa capacità di verifica è fondamentale per soddisfare i requisiti di sicurezza ricercati nell'area EMEA e APAC. Inoltre, Red Hat fornisce software con firma crittografica e provenienza verificata che soddisfano i requisiti delle normative emergenti, come il Regolamento sulla ciberresilienza (CRA) dell'UE.

- **Sovranità operativa e supporto locale**

  Per far fronte ai rischi giurisdizionali, Red Hat supporta la sovranità operativa offrendo alle organizzazioni la possibilità di avere il pieno controllo su chi gestisce l'infrastruttura.

  - **Supporto sovrano:** Come già accennato in precedenza, Red Hat offre un servizio di assistenza sovrano per l'Unione Europea. Il servizio prevede che il supporto tecnico venga fornito esclusivamente da cittadini dell'UE verificati che risiedono entro i confini dell'UE. Questo tipo di supporto garantisce che i dati a cui ha accesso il personale di supporto non lasceranno la regione.
  - **Ecosistemi locali:** Red Hat mette a disposizione un ecosistema di partner locali certificati, tra cui provider di soluzioni cloud che offrono funzionalità di cloud sovrano conformi alle rigide leggi nazionali in materia di residenza.

- **Indipendenza tecnologica**

  Una strategia di cloud ibrido e open source permette di eseguire i carichi di lavoro in un'ampia gamma di ambienti (on premise, in un cloud privato, all'edge della rete o in un ambiente isolato).

- **Portabilità:** Questo è un aspetto chiave per prevenire il vendor lock-in, che è una delle principali preoccupazioni per le agenzie governative, in particolare in regioni come LATAM e APAC. In queste regioni la capacità di trasferire in modo efficiente i carichi di lavoro e i dati è un requisito fondamentale per assicurare la continuità del servizio e la massima reattività ai cambiamenti geopolitici, che potrebbero richiedere il passaggio rapido a un nuovo provider.
- **Operazioni disconnesse:** Le soluzioni Red Hat, come Red Hat Device Edge e Red Hat OpenShift, sono molto indicate per le agenzie di difesa poiché garantiscono il funzionamento autonomo dei sistemi in ambienti DDIL e assicurano la sopravvivenza della missione anche quando il cloud centrale è irraggiungibile.

Red Hat offre alle agenzie governative una base open source per creare un cloud sovrano che resista alle incertezze, tuteli i dati con sistemi affidabili e garantisca l'operatività dell'intera nazione.

- **IA sovrana**

  Oggi che governi ed enti governativi stanno esplorando il potenziale dell'IA, Red Hat offre una piattaforma ideale per creare un'IA sovrana. In questo modo le nazioni possono mantenere la proprietà dei modelli e dei dati per l'addestramento, distribuendoli su infrastrutture localizzate conformi a normative come il Regolamento sull'intelligenza artificiale dell'UE (AI Act), invece di utilizzare modelli gestiti al di fuori della giurisdizione.

Perché scegliere Red Hat nel settore pubblico?

Red Hat è un partner affidabile per le organizzazioni che operano nel settore pubblico, impiegato nel 100% dei dipartimenti esecutivi statunitensi[3] e ampiamente utilizzato da NATO e ministeri della difesa di tutto il mondo. I principi che guidano Red Hat e il suo modello di licenza eliminano del tutto il rischio di vincolarsi alle soluzioni di un singolo fornitore. Le organizzazioni conservano il diritto di utilizzare e gestire il software a tempo indeterminato, proteggendo gli investimenti a lungo termine da eventuali modifiche alle roadmap da parte dei fornitori o da restrizioni geopolitiche.

Con l'aumento della spesa, in particolare nel settore della difesa, investire nel portafoglio di soluzioni e servizi Red Hat può portare un ritorno sull'investimento visibile. Si stima che gli impegni di spesa degli stati membri della NATO raddoppieranno, raggiungendo il 5% del PIL nazionale entro il 2035.[4] L'utilizzo di una piattaforma unificata aiuta a migliorare la standardizzazione di ambienti e processi, riduce significativamente i costi operativi e il costo totale di proprietà. Inoltre, grazie alla nuova uniformità le agenzie potranno destinare il budget prima dedicato alla gestione dei sistemi frammentari allo sviluppo di nuove capacità per le missioni.

Passaggi successivi

- Scopri di più sul contributo di Red Hat al settore pubblico e contatta un esperto di Red Hat per maggiori informazioni.
- Ti interessa capire se la tua organizzazione è davvero pronta a implementare la sovranità digitale? Leggi l'articolo del blog dedicato.

3 Dati relativi a clienti Red Hat, settembre 2025.

4 "Defence expenditures and NATO's 5% commitment", NATO, 18 dicembre 2025.

Informazioni su Red Hat

Red Hat è leader mondiale nella fornitura di soluzioni software open source. Con un approccio basato sul concetto di community, distribuisce tecnologie come Kubernetes, container, Linux e cloud ibrido caratterizzate da affidabilità e prestazioni elevate. Red Hat consente di sviluppare applicazioni cloud native, integrare applicazioni IT nuove ed esistenti, nonché automatizzare e gestire ambienti complessi. Considerata un partner affidabile dalle aziende della classifica Fortune 500, Red Hat fornisce pluripremiati servizi di consulenza, formazione e assistenza, che portano i vantaggi dell'innovazione open source in qualsiasi settore. Red Hat è l'elemento catalizzatore in una rete globale di aziende, partner e community, e permette alle organizzazioni di crescere, evolversi e prepararsi a un futuro digitale.

facebook.com/RedHatItaly
twitter.com/RedHatItaly
linkedin.com/company/red-hat

ITALIA
it.redhat.com
italy@redhat.com

EUROPA, MEDIO ORIENTE, E AFRICA (EMEA)
00800 7334 2835
it.redhat.com
europe@redhat.com

it.redhat.com
#3613114_0326