



Sovranità digitale europea: il controllo dei dati entra nell'agenda geopolitica

Pubblicato il 04/02/2026

Nel nuovo scenario internazionale, **dati e infrastrutture digitali** sono diventati elementi centrali della sicurezza degli Stati. I conflitti recenti, le tensioni geopolitiche e l'evoluzione tecnologica globale hanno accelerato una consapevolezza già presente nelle istituzioni europee: senza il controllo dei sistemi informativi non può esistere una piena **sovranità digitale**.

È in questo contesto che va letta la decisione della Francia di abbandonare Microsoft Teams, Zoom e Google Meet per le comunicazioni ministeriali, sostituendoli con una piattaforma nazionale. La scelta si inserisce in una strategia volta a **rafforzare il controllo pubblico sui flussi informativi sensibili**, riducendo l'esposizione a dipendenze tecnologiche esterne.

Da Berlino a Vienna, da Copenaghen alle capitali dell'Europa centrale, si sta delineando un orientamento comune: la tecnologia è considerata parte integrante della **sicurezza nazionale**, al pari dell'energia e delle infrastrutture critiche. La domanda di fondo è lineare: **chi può accedere ai dati pubblici europei in caso di crisi internazionale?**

La Germania rappresenta uno dei casi più avanzati di questa transizione. Il Land dello Schleswig-Holstein ha completato la migrazione di circa 30.000 dipendenti pubblici da Microsoft Office a LibreOffice e da Windows a Linux. Parallelamente, il Ministero dell'Interno ha lanciato openDesk, una suite basata su componenti open source come Nextcloud, con l'obiettivo di sostituire Microsoft 365 e mantenere i dati amministrativi entro **perimetri giuridici nazionali**.

Non si tratta solo di una scelta economica. Al centro c'è il superamento del *vendor lock-in*, la dipendenza strutturale da un unico fornitore che può rendere complessa la sostituzione di sistemi e servizi. Anche la Bundeswehr ha avviato percorsi verso infrastrutture sovrane, confermando come la protezione del codice, dei metadati e delle comunicazioni sia entrata stabilmente nelle politiche di sicurezza.

Sicurezza nazionale e convergenza normativa

Austria e Danimarca hanno intrapreso percorsi simili. Il Bundesheer austriaco ha rimosso Microsoft Office da 16.000 postazioni militari, mentre le principali città danesi stanno progressivamente abbandonando Office 365, richiamando l'esigenza di garantire la **tutela dei dati scolastici e amministrativi** e una governance più controllabile delle piattaforme digitali.

Il tema è anche giuridico. Da un lato il GDPR europeo, dall'altro l'US Cloud Act, che consente alle autorità statunitensi di richiedere accesso ai dati gestiti da aziende americane anche se archiviati in Europa. Questa tensione normativa è stata evidenziata dalla sentenza Schrems II della Corte di Giustizia UE, che ha imposto limiti stringenti ai trasferimenti verso Paesi extra-UE, richiedendo garanzie effettive per la protezione dei dati.



Palais de l'Europe, Strasburgo – sede del Consiglio d'Europa e della CEPEJ.

Nel settore giudiziario, la CEPEJ ha inserito nel Piano d'Azione di Valletta 2026–2029 il principio della **sovranità dei dati** e dell'uso di intelligenza artificiale open source, per garantire trasparenza degli algoritmi e pieno controllo dei sistemi digitali impiegati nelle corti.

In Italia il quadro normativo è tra i più strutturati. L'articolo 68 del Codice dell'Amministrazione Digitale impone alle pubbliche amministrazioni di privilegiare soluzioni open source o a riuso. Il PNRR ha destinato oltre un miliardo di euro al Polo Strategico Nazionale. Il Ministero della Difesa ha già migrato circa 150.000 postazioni verso LibreOffice, mentre regioni come Emilia-Romagna e Bolzano sono citate come esempi virtuosi. Resta tuttavia una **attuazione non omogenea**, con velocità e modalità diverse tra enti centrali e territoriali.

Tecnologia europea e cooperazione continentale

Le alternative europee e open source sono ormai consolidate. LibreOffice è utilizzato in numerose amministrazioni per la produttività. Nextcloud consente collaborazione cloud su server controllati dallo Stato. Per le videoconferenze si affermano soluzioni open source come Jitsi Meet e BigBlueButton. Per la messaggistica sicura, Element basato su Matrix è già adottato da diversi governi europei.



Digital Europe Programme a Bruxelles: cooperazione istituzionale per infrastrutture digitali europee.

A livello comunitario sono in corso iniziative come Gaia-X, il consorzio EDIC e lo Sovereign Cloud Stack. La Commissione Europea sostiene questo percorso attraverso il Digital Europe Programme, finalizzato a costruire un ecosistema digitale europeo più interoperabile.

La sfida principale resta il coordinamento tra iniziative nazionali, così da preservare **interoperabilità e cooperazione** tra gli Stati membri. In questa prospettiva, la sovranità digitale europea si configura come un processo graduale, fondato su sicurezza, autonomia tecnologica e collaborazione istituzionale, destinato a incidere in modo crescente sulle scelte amministrative e strategiche del continente.

Link notizia: <https://www.altalex.com/documents/news/2026/02/03/sovranita-digitale-europea-quando-tecnologia-diventa-affare-stato>