POLICY BRIEF

Sovranità Digitale nella Pubblica Amministrazione Italiana

Osservatorio Nazionale Sovranità Digitale — Giugno 2025

Il problema

La Pubblica Amministrazione italiana dipende in misura significativa da infrastrutture digitali gestite da provider soggetti a giurisdizioni extra-europee. Questa dipendenza espone le comunicazioni istituzionali e i dati dei cittadini a rischi concreti di accesso da parte di autorità straniere, in particolare attraverso il CLOUD Act statunitense (2018), e si pone in potenziale contrasto con il GDPR e le sentenze della Corte di Giustizia dell'UE (Schrems I e II).

I numeri

- ~23.000 enti PA monitorati (fonte IndicePA)
- I servizi email sono il primo ambito analizzato
- La mappatura copre tutti i domini istituzionali registrati
- I dati sono raccolti e aggiornati tramite analisi automatica dei record MX
- Il dataset è aperto, verificabile e rilasciato sotto licenza CC BY-SA 4.0

Il contesto normativo

Il quadro normativo europeo e italiano impone obblighi precisi sulla localizzazione e protezione dei dati della PA:

Norma	Rilevanza
GDPR (Reg. UE 2016/679)	Vieta trasferimenti dati verso paesi terzi senza garanzie adeguate
Schrems II (CGUE, 2020)	Ha invalidato il Privacy Shield UE-USA
CLOUD Act (USA, 2018)	Consente accesso USA a dati di provider americani anche in UE
Strategia Cloud Italia (2021)	Classifica i dati PA e prevede migrazione verso infrastrutture qualificate
NIS2 (Dir. UE 2022/2555)	Requisiti cybersecurity per PA e soggetti essenziali

Raccomandazioni

1. Censimento obbligatorio dei servizi digitali della PA

Rendere obbligatoria la dichiarazione dei servizi digitali utilizzati da ogni ente e della relativa giurisdizione. Integrare questa informazione nell'IndicePA per renderla pubblica e monitorabile.

2. Requisiti di sovranità nelle convenzioni Consip

Inserire criteri di sovranità digitale (giurisdizione dati, localizzazione server, assenza obblighi verso autorità extra-UE) nelle convenzioni per servizi email e cloud.

3. Piano nazionale di migrazione

Definire un piano con scadenze progressive per la migrazione dei servizi email della PA verso provider conformi. Prevedere fondi dedicati dal PNRR o dalla cybersecurity.

4. Monitoraggio continuo e trasparente

Istituzionalizzare il monitoraggio della sovranità digitale della PA con dati pubblici e aggiornati periodicamente.

5. Promozione del modello a livello europeo

Proporre nelle sedi europee l'adozione di un framework comune per il monitoraggio della sovranità digitale delle PA in tutti gli stati membri.

Cosa puoi fare

Se sei un parlamentare: Presenta un'interrogazione citando i dati dell'Osservatorio. Proponi l'inserimento di requisiti di sovranità nella normativa.

Se sei un dirigente PA: Verifica la posizione del tuo ente e avvia una valutazione interna sulla migrazione.

Se sei un regolatore: Utilizza i dati per aggiornare le linee guida e inserire requisiti nelle convenzioni.

Fonti e riferimenti

- Osservatorio Nazionale Sovranità Digitale: https://osservatorio.mxmap.it/
- MxMap.it — Mappatura provider email PA: https://mxmap.it/
- IndicePA — Indice delle Pubbliche Amministrazioni: https://indicepa.gov.it
- GDPR: Regolamento UE 2016/679
- Sentenza Schrems II: CGUE C-311/18