TECHNICAL BRIEF

Analisi Tecnico-Normativa della Dipendenza Digitale nella Pubblica Amministrazione Italiana

Per AgID, ACN, Garante per la Protezione dei Dati Personali — Osservatorio Nazionale Sovranità Digitale — Giugno 2025

Executive Summary

Il presente documento analizza la dipendenza della Pubblica Amministrazione italiana da infrastrutture di comunicazione digitale gestite da soggetti extra-europei. L'analisi si basa sui dati raccolti dal progetto MxMap.it, che ha mappato i record MX (Mail Exchange) di tutti i domini istituzionali registrati nell'Indice delle Pubbliche Amministrazioni (IndicePA).

I risultati evidenziano una significativa esposizione delle comunicazioni istituzionali a giurisdizioni terze, con implicazioni dirette su: protezione dei dati personali (GDPR, Schrems II), sicurezza nazionale (NIS2, Perimetro di Sicurezza Nazionale Cibernetica), autonomia strategica e conformità alle linee guida AgID e alla Strategia Cloud Italia.

Risultati chiave

- La PA italiana comprende circa 23.000 enti con domini email istituzionali
- Una quota significativa di questi enti utilizza provider email soggetti a giurisdizione extra-UE
- I provider statunitensi sono soggetti al CLOUD Act (18 U.S.C. § 2713, 2018)
- Le comunicazioni istituzionali contengono regolarmente dati personali ex art. 4 GDPR
- La dipendenza è trasversale: Comuni, ASL, Università, Ministeri
- Non esiste attualmente un obbligo di disclosure del provider email nel catalogo IndicePA

Destinatari

Ente	Competenza	Azione attesa
AgID	Linee guida, qualificazione cloud, IndicePA	Aggiornamento linee guida e catalogo IndicePA
ACN	Cybersecurity, Perimetro Sicurezza, NIS2	Valutazione rischio, requisiti sicurezza
Garante Privacy	Protezione dati, trasferimenti extra-UE	Verifica conformità, provvedimenti
ANAC	Trasparenza, procurement pubblico	Requisiti sovranità in gare d'appalto

1. Metodologia di raccolta dati

La metodologia adottata si articola in quattro fasi sequenziali, ciascuna automatizzata e documentata per garantire riproducibilità e verificabilità.

1.1 Acquisizione dell'elenco enti

L'elenco degli enti e dei relativi domini istituzionali viene estratto dall'IndicePA attraverso l'API CKAN JSON. L'IndicePA, gestito da AgID ai sensi dell'art. 6-ter del CAD (D.Lgs. 82/2005), è la fonte autoritativa per l'identificazione di tutte le PA italiane. Vengono estratti: codice IPA (cod_amm), denominazione, dominio email, tipologia ente e regione.

1.2 Risoluzione DNS dei record MX

Per ciascun dominio istituzionale viene effettuata una query DNS di tipo MX (RFC 7208). I record MX indicano i server designati a ricevere la posta elettronica per quel dominio. La risoluzione avviene tramite resolver pubblici per garantire risultati non influenzati da configurazioni locali.

1.3 Identificazione del provider

I record MX vengono confrontati con un database di pattern noti per identificare il provider email. Il database contiene oltre 200 pattern di provider, mantenuto e aggiornato nel repository open source MxMap.it. La classificazione assegna a ogni provider:

- Nome commerciale del provider (es. Google Workspace, Microsoft 365)
- Paese di sede legale dell'operatore (codice ISO 3166-1)
- Classificazione di sovranità: IT (italiano), EU (europeo), EXTRA_EU (extra-europeo)

1.4 Validazione e pubblicazione

I dati aggregati vengono sottoposti a controlli di qualità automatici (coerenza dei codici IPA, validità dei domini, completezza dei record) e pubblicati in formato CSV e JSON sotto licenza CC BY-SA 4.0. L'intero processo è ripetibile e il codice sorgente è pubblicamente disponibile.

Schema dati del dataset

Campo	Tipo	Descrizione	Fonte
cod_amm	string	Codice IPA dell'ente	IndicePA
des_amm	string	Denominazione ufficiale	IndicePA
dominio	string	Dominio email istituzionale	IndicePA
mx_records	string[]	Record MX rilevati	DNS query
provider	string	Provider identificato	MxMap.it
provider_country	ISO 3166	Sede legale del provider	MxMap.it
sovereignty	enum	IT / EU / EXTRA_EU	MxMap.it

2. Quadro normativo di riferimento

La dipendenza da provider extra-UE per le comunicazioni istituzionali interseca molteplici profili normativi, ciascuno con implicazioni specifiche per gli enti e per i regolatori.

2.1 Regolamento Generale sulla Protezione dei Dati (GDPR)

Il GDPR (Reg. UE 2016/679) disciplina il trattamento e il trasferimento dei dati personali. La posta elettronica istituzionale costituisce trattamento di dati personali ai sensi dell'art. 4, in quanto le comunicazioni contengono regolarmente: nomi, indirizzi, codici fiscali, dati sanitari, informazioni giudiziarie e altri dati sensibili.

Il Capo V del GDPR (artt. 44-49) subordina i trasferimenti verso paesi terzi a garanzie specifiche. L'utilizzo di un provider soggetto al CLOUD Act configura un potenziale trasferimento extra-UE indipendentemente dalla localizzazione fisica dei server, poiché l'autorità giudiziaria statunitense può imporre la disclosure dei dati al provider.

Sentenze Schrems I e II — Implicazioni

Schrems I (C-362/14, 2015): La CGUE ha invalidato il Safe Harbor per insufficienza di garanzie contro la sorveglianza di massa USA.

Schrems II (C-311/18, 2020): La CGUE ha invalidato il Privacy Shield e richiesto una valutazione caso per caso delle clausole contrattuali standard (SCC). Le SCC sono insufficienti quando il diritto del paese terzo impone obblighi di disclosure incompatibili con le garanzie europee.

Data Privacy Framework (2023): Decisione di adeguatezza CE per gli USA, ma applicabile solo alle organizzazioni auto-certificate DPF. Non risolve il conflitto strutturale CLOUD Act / GDPR e potrebbe essere invalidata ("Schrems III").

2.2 CLOUD Act (Clarifying Lawful Overseas Use of Data Act)

Il CLOUD Act (18 U.S.C. § 2713, 2018) consente alle autorità giudiziarie statunitensi di richiedere a qualsiasi provider soggetto a giurisdizione USA la produzione di dati in loro possesso, custodia o controllo, indipendentemente dalla localizzazione fisica dei dati.

Questo significa che un ente PA che utilizza Google Workspace o Microsoft 365 per la posta elettronica espone le proprie comunicazioni istituzionali alla potenziale disclosure verso le autorità USA, anche se i server sono fisicamente situati in Europa (regioni UE dei cloud provider).

Conflitto giuridico strutturale

Il CLOUD Act crea un conflitto diretto con il GDPR: il provider è obbligato a produrre i dati dal diritto USA, ma è vietato dal farlo dal diritto UE. Questo conflitto non è risolvibile attraverso misure contrattuali o tecniche, poiché l'obbligo di disclosure del CLOUD Act prevale sugli accordi contrattuali del provider.

2.3 Strategia Cloud Italia e qualificazione ACN

La Strategia Cloud Italia (2021) classifica i dati della PA in tre livelli: ordinari, critici e strategici. Per i dati critici e strategici è prevista la migrazione verso il Polo Strategico Nazionale (PSN) o verso infrastrutture qualificate da ACN (Agenzia per la Cybersicurezza Nazionale).

Il Regolamento ACN per la qualificazione dei servizi cloud per la PA (Determinazione n. 307/2022 e successive modifiche) definisce requisiti specifici per la localizzazione dei dati e il controllo giurisdizionale. I servizi qualificati al livello QC3 (strategico) e QC2 (critico) devono garantire che i dati non siano accessibili da giurisdizioni extra-UE.

2.4 Direttiva NIS2 e D.Lgs. 138/2024

La Direttiva NIS2 (2022/2555), recepita con D.Lgs. 138/2024, impone alle PA obblighi di gestione del rischio cybersecurity, inclusa la valutazione dei rischi della supply chain. La dipendenza da provider email extra-UE configura un rischio di supply chain che deve essere valutato e gestito nell'ambito delle misure di sicurezza previste dall'art. 21.

3. Analisi dei rischi

La dipendenza da provider extra-UE genera rischi su quattro dimensioni interconnesse, ciascuna rilevante per diversi profili regolatori.

Dimensione	Rischio	Impatto	Regolatore
Giurisdizionale	Accesso ai dati PA da parte di autorità extra-UE tramite CLOUD Act o normativa equivalente	ALTO	Garante, ACN
Protezione dati	Non conformità ai requisiti GDPR per i trasferimenti extra-UE (Capo V); potenziale violazione Schrems II	ALTO	Garante
Continuità operativa	Interruzione del servizio per decisioni unilaterali del provider, sanzioni, conflitti geopolitici	MEDIO	AgID, ACN
Strategico	Lock-in tecnologico, perdita di competenze nazionali, dipendenza strutturale da ecosistemi proprietari	MEDIO	AgID, ANAC
Economico	Flussi finanziari verso operatori esteri, mancato sviluppo dell'industria IT nazionale ed europea	MEDIO	ANAC, Consip

3.1 Scenario: richiesta CLOUD Act

Si consideri lo scenario in cui un'autorità giudiziaria USA emette un ordine di produzione (warrant o subpoena) verso un provider che gestisce la posta di enti PA italiani:

1. Il provider è legalmente obbligato a produrre i dati (18 U.S.C. § 2713)
2. Il provider può contestare l'ordine solo se viola un trattato internazionale — attualmente non esiste un executive agreement UE-USA
3. L'ente PA non viene necessariamente informato della disclosure
4. I dati possono includere: comunicazioni interne, dati dei cittadini, informazioni sensibili, atti amministrativi
5. La disclosure viola potenzialmente gli artt. 44-49 GDPR e configura un data breach ai sensi dell'art. 33

3.2 Rischio per tipologia di ente

L'impatto della dipendenza varia per tipologia di ente in funzione della sensibilità dei dati trattati:

Tipologia	Dati sensibili tipici	Rischio
ASL / Ospedali	Dati sanitari, referti, comunicazioni medico-paziente	CRITICO
Comuni	Anagrafe, stato civile, servizi sociali, tributi	ALTO
Forze dell'ordine	Indagini, segnalazioni, dati giudiziari	CRITICO
Università	Dati studenti, ricerca, proprietà intellettuale	MEDIO
Ministeri	Policy, comunicazioni inter-istituzionali, dati classificati	CRITICO
Autorità indipendenti	Segnalazioni, procedimenti, dati riservati	CRITICO

4. Raccomandazioni per i regolatori

4.1 Raccomandazioni per AgID

R1 — Estendere l'IndicePA con informazioni sul provider email

Inserire nell'IndicePA un campo obbligatorio per il provider email e la relativa classificazione di sovranità. Questo consentirebbe un monitoraggio istituzionale continuo e renderebbe l'informazione pubblica e accessibile a tutti gli stakeholder.

R2 — Aggiornare le linee guida sui servizi email

Aggiornare le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici per includere requisiti espliciti di sovranità giurisdizionale per i servizi di posta elettronica istituzionale. Prevedere un periodo di adeguamento proporzionato alla dimensione dell'ente.

R3 — Definire criteri di qualificazione per i servizi email PA

Analogamente alla qualificazione cloud, definire criteri specifici per i servizi email della PA, includendo: giurisdizione del provider, localizzazione dei dati, assenza di obblighi di disclosure verso autorità extra-UE, conformità GDPR certificata.

4.2 Raccomandazioni per ACN

R4 — Includere la dipendenza email nella valutazione del rischio NIS2

Nelle linee guida per l'attuazione della NIS2, includere esplicitamente la dipendenza da provider email extra-UE come fattore di rischio nella valutazione della supply chain. Richiedere ai soggetti essenziali e importanti una dichiarazione del provider email utilizzato.

R5 — Estendere il Perimetro di Sicurezza Nazionale Cibernetica

Valutare l'inclusione dei servizi di posta elettronica degli enti del Perimetro tra i beni ICT soggetti a notifica e a misure di sicurezza rafforzate, con particolare attenzione alla giurisdizione del provider.

4.3 Raccomandazioni per il Garante Privacy

R6 — Provvedimento generale sull'uso di servizi email extra-UE nella PA

Adottare un provvedimento generale, analogo a quello sui cookie (n. 231/2021) o su Google Analytics (n. 224/2022), che chiarisca le condizioni di liceità dell'utilizzo di servizi email gestiti da provider soggetti al CLOUD Act per le comunicazioni istituzionali della PA.

R7 — DPIA obbligatoria per servizi email PA con provider extra-UE

Richiedere una Valutazione d'Impatto (DPIA, art. 35 GDPR) obbligatoria per gli enti PA che utilizzano servizi email gestiti da provider soggetti a giurisdizioni extra-UE, includendo la valutazione del rischio di disclosure ai sensi del CLOUD Act.

5. Roadmap proposta

Si propone un percorso graduale di adeguamento, articolato in tre fasi, che tenga conto delle diverse dimensioni e capacità degli enti.

Fase	Orizzonte	Azione	Responsabile
1. Trasparenza	0-6 mesi	Censimento obbligatorio provider email in IndicePA; pubblicazione dashboard pubblica	AgID
2. Regolazione	6-18 mesi	Aggiornamento linee guida; provvedimento Garante; criteri NIS2; qualificazione email	AgID, ACN, Garante
3. Migrazione	18-36 mesi	Piano nazionale migrazione con fondi dedicati; priorità per enti con dati critici/strategici	PCM, AgID, ACN

5.1 Criteri di priorità per la migrazione

La migrazione dovrebbe essere prioritizzata in base alla sensibilità dei dati trattati e al profilo di rischio dell'ente:

- Priorità 1 (immediata): Enti del Perimetro Sicurezza Nazionale, Forze dell'ordine, Servizi di intelligence, Ministeri
- Priorità 2 (entro 12 mesi): ASL/Ospedali, Autorità indipendenti, Regioni, Grandi Comuni
- Priorità 3 (entro 24 mesi): Università, Enti di ricerca, Province, Comuni medi
- Priorità 4 (entro 36 mesi): Piccoli Comuni, Enti strumentali, altre PA

6. Conclusioni

L'analisi dei dati MxMap.it evidenzia una dipendenza strutturale della PA italiana da provider email soggetti a giurisdizioni extra-europee. Questa dipendenza non è un problema teorico: il CLOUD Act crea un conflitto giuridico concreto con il GDPR, le sentenze Schrems e la Strategia Cloud Italia.

La soluzione richiede un approccio coordinato tra AgID, ACN e Garante Privacy, con azioni concrete su tre fronti: trasparenza (rendere visibile il problema), regolazione (definire requisiti chiari) e migrazione (supportare gli enti nel percorso di adeguamento).

L'Osservatorio Nazionale Sovranità Digitale mette a disposizione dati aperti, metodologia documentata e strumenti replicabili per supportare questo percorso. Il monitoraggio civico è al servizio delle istituzioni e dei cittadini.

Riferimenti normativi e fonti

- GDPR — Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio
- CLOUD Act — Clarifying Lawful Overseas Use of Data Act (18 U.S.C. § 2713, 2018)
- Schrems I — CGUE, C-362/14 (6 ottobre 2015)
- Schrems II — CGUE, C-311/18 (16 luglio 2020)
- Data Privacy Framework — Decisione di adeguatezza CE (10 luglio 2023)
- Direttiva NIS2 — Direttiva (UE) 2022/2555; D.Lgs. 138/2024
- Strategia Cloud Italia — Dipartimento per la trasformazione digitale (2021)
- CAD — D.Lgs. 82/2005, art. 6-ter (IndicePA)
- Regolamento ACN — Determinazione n. 307/2022 (qualificazione cloud PA)
- Perimetro di Sicurezza Nazionale Cibernetica — D.L. 105/2019, conv. L. 133/2019
- MxMap.it — https://mxmap.it/
- IndicePA — https://indicepa.gov.it
- Osservatorio Nazionale Sovranità Digitale — https://osservatorio.mxmap.it/