Il trattamento dei dati nel Cloud della PA: novità normative, giurisprudenziali e regolamentari

Avv. Prof. Fulvio Sarzana di S.Ippolito, Università LUM e Uninettuno

www.lidis.it

AGID Agenzia per l'Italia Digitale

UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale

Agenzia per la Coesione Territoriale

Presidenza del Consiglio dei Ministri
Dipartimento della Funzione Pubblica

PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020

Il Cloud della PA: i profili strategici ed organizzativi e le norme.

Dalla strategia per la Crescita digitale del Paese, all'adozione del cloud computing nella Pubblica Amministrazione secondo quanto previsto dal Piano Triennale per l'Informatica e, in via indiretta, dall'art 68 del CAD, sino all'art 35 del DL semplificazioni.

Cloud e decreto semplificazioni

L'art. 35 del DL semplificazioni (decreto-legge 16 luglio 2020, n. 76 come convertito nella legge 11 settembre 2020, n 120) intervenendo sull'art. 33-septies della legge n. 221/2012 introduce l'obbligo per le pubbliche amministrazioni centrali di migrare i loro Centri elaborazione dati (Ced), che non hanno i requisiti di sicurezza fissati dall'Agenzia per l'Italia digitale (AgID), verso un'infrastruttura ad alta affidabilità, localizzata in Italia, il cui sviluppo è promosso dalla Presidenza del Consiglio. In alternativa le amministrazioni centrali possono far migrare i loro servizi verso soluzioni cloud per la Pubblica Amministrazione che rispettano i principi stabiliti dall'AgID. Lo stesso obbligo viene previsto per le amministrazioni locali che sono tenute a trasferire i propri servizi nella infrastruttura promossa dalla Presidenza del Consiglio o in altra infrastruttura presente sul territorio e in possesso dei requisiti di sicurezza. In alternativa le amministrazioni locali, come quelle centrali, possono trasferire i propri servizi digitali verso soluzioni cloud per la Pubblica Amministrazione, nel rispetto dei requisiti fissati dall'AgID.

Il ruolo di AGID

Art 35 DL semplificazioni.
L'AgID, con proprio regolamento, d'intesa con la competente struttura della Presidenza del Consiglio dei ministri……
stabilisce i livelli minimi di sicurezza, capacita' elaborativa, risparmio energetico e affidabilita' delle infrastrutture digitali per la pubblica amministrazione, ivi incluse le infrastrutture di cui ai commi 1 e 4-ter. Definisce, inoltre, le caratteristiche di qualita', di sicurezza, di performance e scalabilita', interoperabilita', portabilita' dei servizi cloud per la pubblica amministrazione.

Il ruolo di AGID prima del DL semplificazioni

Le disposizioni di dettaglio, in particolare sulla qualificazione dei servizi SaaS e CSP sono contenute nelle Circolari AgID n. 2 e n. 3 del 9 aprile 2018 e nella la Determinazione n. 419/2020 del 22 settembre 2020.

Le disposizioni citate rispondono agli obiettivi strategici del programma di abilitazione al cloud della PA contenuti nel Piano Triennale per l'informatica 2020-2022.

Il Cloud first

In base al principio *Cloud First*, le PA in fase di definizione di un nuovo progetto, e/o sviluppo di nuovi servizi, devono, in via prioritaria, adottare il paradigma cloud in particolare i servizi SaaS, prima di qualsiasi altra opzione tecnologica, in coerenza con il modello Cloud della PA e le linee guida su acquisizione e riuso di software per le pubbliche amministrazioni (anche alla luce dell'art 68 del CAD) .

Per *Cloud First* si intende, quindi, anche la necessità di ricorrere a strumenti e tecnologie di tipo cloud, nelle sue diverse articolazioni IaaS, PaaS e SaaS, nel momento in cui le pubbliche amministrazioni intendono acquisire sul mercato nuove soluzioni e servizi ICT per la realizzazione di un nuovo progetto o nuovi servizi destinati a cittadini, imprese o utenti interni alla PA.

https://docs.italia.it/italia/piano-triennale-ict/cloud-docs/it/stabile/cloud-enablement.html#il-principio-cloud-first

Il Cloud nel CAD

Art. 68 CAD. Analisi comparativa delle soluzioni

1. Le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato:
2. .....
3. d) software fruibile in modalità cloud computing;
4. Preferenza per c) garanzie del fornitore in materia di livelli di sicurezza, conformità alla normativa in materia di protezione dei dati personali, livelli di servizio tenuto conto della tipologia di software acquisito.

Localizzazione e trattamento dei dati nel Cloud della PA, in particolare per quanto attiene ai criteri di qualificazione adottati da Agid

I criteri di qualificazione adottati da AgID non escludono che un fornitore possa, al fine dell'erogazione del servizio in cloud, trasferire i dati al di fuori dell'Unione Europea, richiedendo unicamente che ciò venga espressamente dichiarato in sede di qualifica unitamente all'indicazione dell'esistenza o meno di accordi circa la protezione dei dati personali tra la UE ed il Paese destinatario

Tuttavia la **localizzazione degli apparati** al di fuori del territorio dell'Unione Europea potrebbe rendere più difficoltoso lo svolgimento di controlli ed audit, e necessitare tutele supplementari.

Ciò significa:

A) bisognerà valutare attentamente, anche in base a quanto previsto dall'art 68 del CAD, il fornitore del Cloud.

B) dovranno eventualmente essere inserite apposite previsioni contrattuali che consentano di avvalersi di soggetti terzi per tali controlli, eventualmente prevedendo che i costi siano sopportati dal fornitore.

Localizzazione Extra-Ue

il Regolamento (UE) n. 679/2016 sulla protezione dei dati personali (**Gdpr**) disciplina in maniera stringente le possibilità di **trasferimento dei dati in Paesi extra-UE**, prevedendo la necessaria esistenza di misure di garanzia adeguate.

E' opportuno, pertanto, che in tali ipotesi vengano previsti appositi meccanismi di "migrazione" dei dati al fine di agevolarne il rientro all'interno della UE qualora vengano meno i presupposti di adeguatezza, soprattutto se ciò derivi da una decisione della Corte di Giustizia.

La dipendenza della PA dai fornitori extra UE.

Attualmente, il mercato mondiale dei principali fornitori di infrastrutture cloud è dominato da cinque gruppi societari, quattro dei quali (Amazon, Microsoft, Google, IBM) hanno la sede principale negli Stati Uniti, il quinto, Alibaba, in Cina. Quote residuali del mercato sono distribuite tra ulteriori gruppi, prevalentemente con base nordamericana (es. Cisco Systems, Salesforce, Oracle) esclusi alcuni gruppi europei.

La pronuncia Schrems II della Corte di Giustizia

La recente pronuncia cd. “Schrems II” della Corte di Giustizia Europea e, in precedenza, sia pure con inferiore perimetro di interesse per il vasto pubblico, i risultati dello studio congiunto EDPB-EDPS sul Cloud Act statunitense hanno posto con forza il problema del trasferimento extra-UE di flussi di dati personali e delle connesse garanzie.

La Corte di giustizia nel caso Schrems II

la Corte di Giustizia UE nella pronuncia richiamata che invalida il privacy shield, si sofferma soprattutto su due fonti normative, la Section 702 del Foreign Intelligence Surveillance Act (FISA) e l'E.O. 12333 (cfr. sentenza cit., § 60 e ss.).

La responsabilità dei fornitori di servizi cloud in materia di trattamento dei dati

I fornitori che trattano dati extra UE dovranno dunque prestare sufficienti garanzie che i dati non vengano diffusi in base ad attività di sorveglianza extra UE per finalità di intelligence, e dunque, ad esempio è responsabilità della società potenzialmente soggetta al *Cloud Act* dare sufficienti garanzie circa la conformità del trattamento al GDPR.

Cloud e protezione dei dati personali

Il contratto di fornitura di servizi cloud dovrà poi essere accompagnato dall'atto con cui vengono disciplinati in capo al fornitore i vari obblighi previsti dall'art. 28 del Regolamento (UE) n. 679/2016.

E' indubbio, infatti, che tale fornitore nell'erogazione del servizio riveste il ruolo di Responsabile del trattamento, e come tale assumerà gli obblighi ed i vincoli stabiliti dalla normativa a protezione dei dati personali.

Attenzione che la PA deve fornire al responsabile precise indicazioni sul contenimento dei rischi legati alla sicurezza dei dati personali.

Si pensi alle ipotesi di trattamento di dati inerenti alla salute o altri dati rientranti tra quelle particolari categorie di cui all'art. 9 del Regolamento.

In questi casi l'amministrazione, con il supporto del fornitore dovrà individuare misure di sicurezza adeguate, che il fornitore dovrà implementare rimanendo, in assenza di istruzioni da parte del Titolare, esonerato da eventuali responsabilità.

GRAZIE!!!!