STRATEGIE CLOUD ITALIA

18 NOVEMBRE 2022 REDAZIONE LASCIA UN COMMENTO

di Michele IASELLI

La strategia Cloud Italia ha un ruolo centrale nella digitalizzazione della PA, priorità del PNRR: l'obiettivo è semplificare il lavoro delle pubbliche amministrazioni, oltre ad adottare tecnologie sicure e garantire la compliance normativa, anche al GDPR

La digitalizzazione della PA si impone oggi come obiettivo prioritario del PNRR per garantire ai cittadini e alle imprese servizi pubblici di maggiore qualità, efficienza ed efficacia, oltre che per creare nuove opportunità di sviluppo per l'economia digitale del Paese. In questo processo di trasformazione, la **strategia Cloud Italia** riveste un ruolo centrale e, in continuità con le iniziative previste nel piano nazionale, introduce importanti novità al fine di semplificare il lavoro delle amministrazioni.

Mediante l'approccio cloud first, la strategia intende guidare e favorire l'adozione sicura, controllata e completa delle tecnologie cloud da parte del settore pubblico, **in linea con i principi di tutela della privacy** e con le raccomandazioni delle istituzioni europee e nazionali. In tal modo le infrastrutture digitali saranno più affidabili e sicure, e la PA potrà rispondere in maniera organizzata agli attacchi informatici, garantendo continuità e qualità nella fruizione di dati e servizi.

Indice degli argomenti

Strategia cloud Italia, le tre direttrici

Tre le sfide che la Strategia Cloud Italia intende affrontare c'è assicurare l'autonomia tecnologica del Paese, oltre a garantire il controllo sui dati e aumentare la resilienza dei servizi digitali. La strategia, infatti, si sviluppa **secondo tre direttrici** che guideranno gli enti nelle scelte da compiere rispetto alle diverse soluzioni di migrazione al cloud. Vediamo le tre direttrici della Strategia Cloud Italia

- Consente l'invio di comunicazioni promozionali inerenti i prodotti e servizi di soggetti terzi rispetto alle Contitolari che appartengono al ramo manifatturiero, di servizi (in

particolare ICT) e di commercio, con modalità di contatto automatizzate e tradizionali da parte dei terzi medesimi, a cui vengono comunicati i dati.

Classificare dati e servizi della PA per guidare e supportare la migrazione al cloud

L'ampio spettro dei servizi Cloud disponibili, alla luce delle sfide tecnologiche e normative presentate, deve essere adottato in modo regolamentato così da mitigare i rischi sistemici dell'adozione del Cloud. L'elemento fondamentale per tale regolamentazione **è individuare un processo sistematico** di classificazione dei dati e dei servizi gestiti dalle PA, il cui risultato possa essere utilizzato per uniformare e guidare il processo di migrazione al Cloud della PA. Le classi dei dati e servizi sono identificate sulla base del danno che una loro compromissione, in termini di confidenzialità, integrità e disponibilità, provocherebbe al sistema Paese. Tali classi sono:

- **Strategico**: dati e servizi la cui compromissione può avere un impatto sulla sicurezza nazionale;
- **Critico**: dati e servizi la cui compromissione potrebbe determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale del Paese;

- **Ordinario**: dati e servizi la cui compromissione non provochi l'interruzione di servizi dello Stato o, comunque, un pregiudizio per il benessere economico e sociale del Paese.

Questa classificazione **astrae da specifiche normative** e requisiti di sicurezza descrivendo esclusivamente l'impatto per il sistema Paese di una eventuale compromissione di certi dati e servizi. L'applicazione del processo di classificazione, di seguito definito, permetterà un'analisi guidata degli impatti, nonché di eventuali requisiti di sicurezza e normativi, per l'identificazione dell'opportuna classe. Ad esempio, i dati e servizi afferenti funzioni essenziali dello Stato, ovvero identificati nell'ambito del PSNC, saranno classificati come strategici, i dati sanitari dei cittadini saranno classificati come critici, mentre dati e servizi relativi a portali istituzionali delle amministrazioni saranno classificati come ordinari.

Qualificare i servizi cloud attraverso un processo di scrutinio tecnologico

L'acquisizione di servizi Cloud da parte delle pubbliche amministrazioni avviene mediante procedure di acquisto la cui scarsa flessibilità difficilmente permette di tenere il passo del mercato e, soprattutto, **di valutare gli effettivi rischi tecnici e organizzativi connessi all'adozione di uno specifico servizio**. Nella prospettiva di facilitare e guidare l'implementazione della policy "Cloud-First" per la PA, risulta dirimente offrire un servizio

di qualificazione ex-ante dei servizi Cloud acquistabili dalla PA. Tale qualificazione, partendo dall'esperienza maturata da AgID, si pone l'obiettivo di semplificare e regolamentare, sia dal punto di vista tecnico che amministrativo, l'adozione di servizi Cloud. Alla luce della classificazione proposta e delle sfide poste dall'adozione del Cloud, la qualificazione dei servizi Cloud non potrà prescindere dall'analisi dei seguenti aspetti:

- gestione operativa dei servizi Cloud, con dettaglio sugli standard tecnico-organizzativi applicati e sulle misure di controllo sui dati;
- requisiti di sicurezza applicati nella gestione dei dati ed erogazione di servizi, quali le modalità di gestione delle chiavi di cifratura e i controlli di sicurezza applicati;
- condizioni contrattuali applicate all'erogazione del servizio (Service-Level Agreement, SLA) e alla sua rendicontazione, quali le garanzie di disponibilità e altri strumenti contrattuali a disposizione delle amministrazioni.

Sulla base dell'analisi delle soluzioni tecnologiche e organizzative disponibili sul mercato, i tre aspetti di analisi permettono di individuare a priori la qualificazione dei servizi Cloud riportata di seguito:

- I **servizi di Cloud Pubblico non qualificato** (extra UE/UE), ovvero quei servizi che non rispondono ai criteri tecnico-organizzativi e normativi individuati in precedenza.
- I **servizi di Cloud Pubblico qualificato** (UE) compatibili con legislazioni rilevanti in materia (es. GDPR e NIS) che consento la localizzazione dei dati in UE e il rispetto di requisiti di sicurezza tecnico organizzativi, tipicamente sulla base di sistemi di cifratura granulare gestiti dal fornitore CSP.

- I **servizi di Cloud pubblico** con controllo on-premise dei meccanismi di sicurezza, c.d. Cloud Pubblico Criptato (IT), che consentono di incrementare significativamente il livello di controllo sui dati e servizi, introducendo un maggior livello di autonomia dai CSP extra-UE nella gestione operativa e il controllo delle infrastrutture tecnologiche.
- **Soluzioni di Cloud privato e ibrido**, infine, permettono la localizzazione dei dati in Italia e maggior isolamento dalle regioni pubbliche dei principali CSP. Tali garanzie di autonomia sono ottenute mediante la gestione operativa da parte di un fornitore soggetto a vigilanza e monitoraggio pubblico. Queste implementazioni si possono distinguere tra:

1. **soluzioni basate su tecnologia hyperscaler licenziata da uno o più CSP**, c.d. Cloud privato/ibrido "su licenza" (IT), oppure
2. **soluzioni basate su tecnologie commerciali** qualificate mediante procedure di scrutinio e certificazione tecnologica, c.d. Cloud Privato Qualificato (IT).

I servizi Cloud qualificati potranno essere utilizzati, in accordo alla classificazione dei dati, con i seguenti vincoli:

- le offerte di **Cloud Pubblico Qualificato e Pubblico Criptato**, potranno ospitare dati e servizi ordinari
- le offerte di **Cloud Pubblico Criptato, Privato/Ibrido** "su licenza" e Privato Qualificato potranno ospitare dati e servizi critici;
- le offerte di **Cloud Privato/Ibrido** "su licenza" e Privato Qualificato potranno ospitare dati e servizi strategici.

Questo processo di adozione dei servizi Cloud nella PA, dovrà culminare con la realizzazione di un mercato elettronico dei servizi Cloud qualificati. Tale mercato dovrà rappresentare il mezzo mediante il quale le amministrazioni saranno guidate, in accordo al processo di classificazione dei dati e dei servizi, nella scelta dei servizi Cloud per loro più idonei e all'acquisto diretto con strumenti amministrativi semplificati e pre-negoziati.

Realizzare il PSN dedicato ai servizi strategici, sotto controllo ed indirizzo pubblico

Lo sviluppo di una nuova infrastruttura informatica a servizio della PA localizzata sul territorio nazionale, il Polo Strategico Nazionale(PSN). Il PSN ha infatti l'obiettivo di dotare la PA di tecnologie e infrastrutture Cloud che possano beneficiare delle più alte garanzie di **affidabilità, resilienza e indipendenza**. A tal fine, si prevede che il PSN sia distribuito geograficamente sul territorio nazionale presso siti opportunamente identificati, al fine di garantire adeguati livelli di continuità operativa e tolleranza ai guasti. La gestione operativa del PSN, sarà affidata a un fornitore qualificato sulla base di opportuni requisiti tecnico-organizzativi. Il fornitore dovrà garantire il controllo sui dati in conformità con la normativa in materia, nonché rafforzare la possibilità della PA di negoziare adeguate condizioni contrattuali con i fornitori di servizi Cloud.

Il PSN dovrà permettere alla PA di garantire, sin dalla progettazione (by-design), il rispetto dei **requisiti in materia di sicurezza**, ad esempio PSNC e NIS, e di abilitare la migrazione, almeno inizialmente con un processo lift-and-shift, verso tipologie di servizi Cloud IaaS e PaaS. In accordo alla classificazione fornita nella sezione precedente, il PSN offrirà servizi di Cloud Pubblico Criptato (IT), ovvero permetterà di gestire, ad esempio, strumenti di cifratura on-premise integrati su Cloud pubblico per la PA, e offrirà lo spettro di servizi Cloud privato/ibrido, ovvero il Cloud Privato/Ibrido "su licenza" (IT), il Cloud Privato Qualificato (IT).

A tendere, l'obiettivo del PSN, in accordo alle procedure di classificazione e qualificazione, è di offrire supporto alle amministrazioni centrali e alle principali amministrazioni locali, ad esempio Regioni, ASL e città metropolitane. Ma la strategia cloud del nostro paese deve ovviamente tener conto delle **non poche problematiche che possono sorgere sul fronte della protezione dei dati personali** e tale aspetto implica la necessità di curare con particolare attenzione la policy privacy di tali contratti che descrive l'approccio del fornitore in merito alle informazioni personali del fruitore del servizio.

La normativa di riferimento

Già il **Gruppo di lavoro ex articolo 29** per la protezione dei dati personali, con il parere 05/2012 su cloud computing, ha delineato, a suo tempo, una serie di obblighi di protezione dei dati personali nella relazione cliente-fornitore. In particolare la legittimità del trattamento di dati personali in servizi di cloud computing dipende dall'osservanza di principi fondamentali della legislazione UE in materia di protezione dei dati: dev'essere garantita la trasparenza nei confronti degli interessati, dev'essere rispettato il principio della specificazione e limitazione delle finalità e i dati personali devono essere cancellati non appena la loro conservazione non è più necessaria. Inoltre, devono essere attuate opportune misure tecniche e organizzative per garantire un livello adeguato di protezione e sicurezza dei dati. Oggi, **con il GDPR**, crescono gli obblighi sul trattamento dei dati personali a cui sono tenute le società di cloud. Tra essi rientrano:

- La realizzazione di Misure di sicurezza ex art. 32 GDPR;
- La nomina a responsabile del trattamento ex art. 28 GDPR;
- La nomina di un DPO ex artt. 37-38-39 GDPR;
- Il rispetto dei principi di accountability e privacy by design e by default.

Il valore della trasparenza

La **trasparenza è fondamentale per il trattamento equo e legittimo dei dati personali**. Già la direttiva 95/46/CE, sostituita dal GDPR, obbligava il cliente cloud a fornire all'interessato, presso il quale raccoglie dati che lo riguardano, informazioni sulla sua identità e sulla finalità del trattamento. Il cliente cloud è inoltre tenuto a fornire ulteriori informazioni, ad esempio relative ai destinatari o alle categorie di destinatari dei dati, che possono anche comprendere autorizzati al trattamento nella misura in cui tali ulteriori informazioni siano necessarie per garantire un trattamento leale nei confronti dell'interessato. La trasparenza dev'essere garantita anche nel rapporto tra cliente cloud, fornitore cloud e (eventuali) subcontraenti. Il cliente cloud è in grado di valutare la legittimità del trattamento di dati personali nei servizi cloud solo se il fornitore del servizio lo informa in merito a tutte le questioni pertinenti.

Un titolare del trattamento che preveda di ingaggiare un fornitore cloud dovrebbe verificare attentamente i termini e le condizioni di tale fornitore e valutarli dal punto di vista della protezione dei dati. Ai fini della **trasparenza nel cloud computing** occorre che il cliente cloud sia a conoscenza di tutti i subcontraenti che contribuiscono all'erogazione del servizio cloud, nonché dell'ubicazione di tutti i centri presso i quali può essere effettuato il trattamento dei dati personali. Il principio della specificazione e limitazione delle finalità richiede che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità.

Il cliente *cloud* deve determinare la finalità del trattamento prima di procedere alla raccolta di dati personali dall'interessato, informandolo in proposito. Il cliente *cloud* non deve trattare dati personali per finalità diverse che non siano compatibili con quelle originali. Inoltre, occorre garantire che i dati personali non siano (illegalmente) trattati per ulteriori finalità dal fornitore del servizio *cloud* o da uno dei suoi subcontraenti.

I subcontraenti

Poiché un tipico scenario di servizi *cloud* può facilmente **coinvolgere un maggior numero di subcontraenti**, il rischio del trattamento di dati personali per ulteriori finalità incompatibili dev'essere considerato particolarmente alto. Per ridurre al minimo tale rischio, il contratto tra fornitore e cliente *cloud* dovrebbe prevedere misure tecniche e organizzative intese a mitigarlo e fornire garanzie in merito alla registrazione (*logging*) e all'*audit* di operazioni di trattamento di dati personali eseguite da dipendenti del fornitore *cloud* o subcontraenti.

Il contratto dovrebbe prevedere sanzioni contro il fornitore o il subcontraente in caso di violazione della legislazione sulla protezione dei dati.

Conservazione e cancellazione dei dati

Inoltre i dati personali devono essere conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. I dati personali che **non sono più necessari devono essere cancellati o resi anonimi**. Ove non sia possibile cancellarli a causa di norme di legge sulla conservazione (ad es. normative fiscali), l'accesso a tali dati personali dev'essere bloccato. Spetta al cliente cloud garantire che i dati personali siano cancellati non appena non siano più necessari nel senso sopra indicato.

Il **principio della cancellazione dei dati** si applica ai dati personali a prescindere dal fatto che siano memorizzati su disco rigido o altri supporti per la conservazione dei dati (ad es. nastri per backup). Poiché i dati personali possono essere conservati in sovrabbondanza su diversi server in diversi luoghi, occorre garantire che in ciascun caso siano cancellati in modo irrecuperabile (vale a dire che devono essere cancellati anche versioni precedenti, file temporanei e persino frammenti di file).

I clienti cloud devono essere consapevoli del fatto che **i dati di log** che agevolano la verifica, la conservazione, la modifica o la cancellazione dei dati possono anch'essi essere qualificati come dati personali relativi all'interessato che ha avviato la relativa operazione

di trattamento.

La cancellazione sicura dei dati personali impone che i supporti di memorizzazione vengano distrutti o smagnetizzati o che i dati personali conservati siano effettivamente cancellati mediante sovrascrittura. Per la sovrascrittura di dati personali si dovrebbero utilizzare speciali strumenti *software* che sovrascrivono più volte i dati, conformemente a specifiche riconosciute. Il cliente *cloud* dovrebbe assicurarsi che il fornitore *cloud* garantisca **la cancellazione sicura** nel senso sopra citato e che il contratto tra il fornitore e il cliente contenga chiare disposizioni per la cancellazione dei dati personali. Lo stesso vale per i contratti tra fornitori *cloud* e subcontraenti.

La disponibilità e l'integrità nel cloud

In un contratto di cloud in aggiunta agli obiettivi di sicurezza fondamentali, quali disponibilità, riservatezza e integrità, occorre prestare attenzione anche agli obiettivi complementari quali isolamento, possibilità di intervento, responsabilità e portabilità. **Garantire la disponibilità significa assicurare un accesso tempestivo e affidabile ai dati personali.** Una grave minaccia alla disponibilità nel *cloud computing* è la perdita accidentale di connettività di rete tra il cliente e il fornitore o il malfunzionamento del *server* provocato da atti dolosi quali attacchi DoS (Denial of Service) distribuiti.

Altri **rischi per la disponibilità** comprendono guasti accidentali dell'*hardware* sulla rete e nei sistemi *cloud* di trattamento e conservazione dei dati, interruzioni di corrente e altri problemi infrastrutturali. L'integrità si può definire come la proprietà per cui i dati sono autentici e non sono stati alterati intenzionalmente o accidentalmente durante il trattamento, l'archiviazione o la trasmissione. Il concetto di integrità si può estendere ai sistemi informatici e richiede che il trattamento dei dati personali in tali sistemi resti inalterato.

L'importanza della crittografia

Le **alterazioni ai dati personali si possono individuare con meccanismi di autenticazione crittografica**, quali codici di autenticazione di messaggi o firme. Le interferenze nell'integrità dei sistemi informatici nel *cloud computing* si possono impedire o individuare mediante sistemi per l'identificazione/prevenzione di intrusioni (IPS / IDS). Si tratta di un aspetto particolarmente importante nel genere di ambienti di reti aperte dove operano di norma i servizi *cloud*.

In un ambiente cloud, la cifratura può contribuire in misura significativa alla riservatezza dei dati personali, se attuato correttamente, benché non li renda anonimi in modo irreversibile. Si dovrebbe ricorrere alla cifratura dei dati personali in tutti i casi di dati "in

transito" e quando disponibile per dati "a riposo". In alcuni casi (ad es., un servizio di archiviazione IaaS) un cliente cloud può scegliere di non affidarsi a una soluzione di **cifratura offerta dal fornitore cloud**, ma di criptare i dati personali prima di inviarli al sistema cloud. La cifratura dei dati a riposo richiede una particolare attenzione per la gestione della chiave crittografica, poiché la sicurezza dei dati in ultima analisi dipende dalla riservatezza delle chiavi di cifratura.

Le comunicazioni tra fornitore e cliente di servizi cloud e tra centri di trattamento dati **dovrebbero essere criptate**. La gestione a distanza della piattaforma cloud dovrebbe avvenire esclusivamente tramite un canale di comunicazione sicuro. Se un cliente prevede non solo di archiviare, **ma anche di procedere all'ulteriore trattamento dei dati** nel sistema cloud (ad es., consultando schede in banche dati) deve tenere presente che la cifratura dei dati non può essere mantenuta durante il trattamento (tranne per calcoli molto specifici). Ulteriori misure tecniche intese a garantire la riservatezza comprendono i meccanismi di autorizzazione e autenticazione (ad es. l'autenticazione a due fattori). Le clausole contrattuali dovrebbero anche imporre obblighi di riservatezza ai dipendenti di clienti cloud, fornitori cloud e subcontraenti.

Condivisione e interoperabilità

Nelle infrastrutture *cloud*, **risorse quali dispositivi di archiviazione, memorie e reti sono condivise da molti utenti**, con la conseguenza di nuovi rischi di divulgazione e trattamento dei dati per scopi illegittimi. L'obiettivo di protezione "isolamento" è inteso ad affrontare questo aspetto e a contribuire a garantire che i dati non vengano utilizzati al di là delle finalità iniziali e a mantenere la riservatezza e l'integrità. L'isolamento richiede innanzi tutto una *governance* adeguata dei diritti e dei ruoli per l'accesso ai dati personali, verificata su base periodica. Si dovrebbe evitare l'attribuzione di ruoli con privilegi eccessivi (ad esempio, nessun utente o amministratore dovrebbe essere autorizzato ad accedere all'intero sistema *cloud*).

Più in generale, amministratori e utenti devono poter accedere esclusivamente alle informazioni necessarie per le loro finalità legittime (principio del privilegio minimo). In secondo luogo, **l'isolamento dipende anche da misure tecniche** quali l'*hardening* di ipervisori e la gestione corretta di risorse condivise, se si utilizzano macchine virtuali per condividere risorse fisiche tra diversi client *cloud*.

Infine va osservato che attualmente, la maggior parte dei fornitori di servizi *cloud* non utilizzano **formati di dati standard** e interfacce che facilitano l'interoperabilità e la portabilità tra diversi fornitori. Se un cliente *cloud* decide, quindi, di migrare da un fornitore ad un altro, questa mancanza di interoperabilità può rendere impossibile, o comunque molto difficoltoso, trasferire i dati (personali) del cliente al nuovo fornitore *cloud* (il cosiddetto *vendor lock-in*). Lo stesso vale per i servizi sviluppati dal cliente su una

piattaforma offerta dal fornitore originario (PaaS). Prima di ordinare un servizio *cloud,* il cliente *cloud* dovrebbe controllare se e come il fornitore garantisce la portabilità di dati e servizi.