



AWARE

Febbraio 2022*

Strategia Cloud Italia

La migrazione della PA in un
contesto globale/europeo

*I contenuti del paper sono stati ultimati a fine Novembre 2021

AUTORI

Sofia Brunelli
Grazia Menna
Valentino Grassi

CURATORI

Edoardo Crivellaro
Alice Grieco
Alessia Baccani

SI RINGRAZIA

Svetlana Falconi

INDICE

1. Introduzione	p. 1
1.1. Viaggiare nel digitale	p. 1
2. La cronologia del cloud per la Pubblica Amministrazione	p. 3
2.1. Il Sistema Pubblico di Connettività e la gara SPC cloud lotto 1	p. 3
2.2. Il Piano Triennale per l'informatica nella PA 2017-2019	p. 5
2.3. Le circolari AgID 2 e 3 del 2018	p. 7
2.4. Il Piano Triennale per l'informatica nella PA 2019 - 2021	p. 8
2.5. L'articolo 35 del Decreto Legge semplificazioni del 2020	p. 10
2.6. La strategia per il cloud nazionale del Governo Conte II	p. 11
3. Presentazione della Strategia Cloud Italia	p. 14
3.1. Il processo di classificazione dei dati	p. 15
3.2. Il processo di qualificazione dei servizi cloud	p. 15
3.3. Il Polo Strategico Nazionale	p. 17
3.4. Il futuro delle infrastrutture esistenti	p. 18
4. Un Cloud Nazionale Italiano: opportunità, rischi e punti interrogativi	p. 20
4.1. Quali opportunità	p. 20
4.2. Rischi	p. 22
4.3. Punti interrogativi	p. 25
5. Quale cloud per la Pubblica Amministrazione	p. 26
5.1. AWS govcloud (US) e il caso statunitense	p. 27
6. La strategia francese	p. 29
7. Proposte di policy	p. 34
7.1. Inserire la Strategia Cloud Italia all'interno di un approccio olistico	p. 34
7.2. Competenze digitali	p. 36
7.3. Il nodo dell'inter-operabilità	p. 37
8. Conclusioni	p. 38
Bibliografia	p. 39
Contatti	

ABSTRACT

Il paper ha l'obiettivo di inserire la **Strategia Cloud Italia**, presentata qualche mese fa dal governo Draghi, all'interno di un quadro più ampio sul tema del Cloud computing. L'analisi, infatti, si focalizza sulle infrastrutture e strategie che hanno preceduto quella attuale partendo dal *Sistema Pubblico di Connettività* (SPC), passando per i due piani triennali per l'informatica nella Pubblica Amministrazione 2017-2019 e 2019-2021, fino ad arrivare all'articolo 35 del decreto semplificazioni 2020 e alla strategia delineata nella prima bozza del PNRR presentata dal governo Conte II. Alla luce di ciò, e delle infrastrutture già esistenti, ci si è chiesti quali di esse possano essere perpetuate nella Strategia Cloud Italia. Inoltre, il paper accenna i motivi per cui la **Pubblica Amministrazione**, o più in generale un governo, dovrebbe scegliere (o meno) un determinato tipo di cloud; questo dovrebbe avvenire non solo in base alla ponderazione di rischi e benefici ma soprattutto in base alle necessità del soggetto.

1. INTRODUZIONE

1.1. Viaggiare nel digitale

Italia, 1950. Il boom economico spingeva merci e persone a spostarsi con mezzi privati. Negli anni, questo cambiava radicalmente il modo di concepire la mobilità stessa: nasceva la necessità di nuove infrastrutture in grado di mettere in collegamento tra loro città e le imprese, aziende e industrie con i lavoratori che vi prestavano la loro opera.

Le **autostrade** divennero i nuovi fulcri della viabilità e dell'economia.



Italia, 2021. L'economia non corre più in autostrada, ma viaggia nel **digitale**. Complice l'emergenza sanitaria innescata dal COVID-19, quella della *digital transformation* è diventata una necessità più che un'opzione. Pur trattandosi di un cambiamento drastico e trasversale, alcuni settori hanno risentito in modo sempre più radicale e repentino di questa "metamorfosi". Tra questi, spiccano quello della sanità e della pubblica amministrazione. Il mondo sanitario si è trovato infatti a dover improvvisamente garantire assistenza virtuale a milioni di cittadini, segnando così l'ascesa della *telemedicina*.



Per quanto concerne la **pubblica amministrazione**, invece, l'Agenda Digitale ha posto tra i suoi obiettivi principali quello di *incentivare la crescita economica tramite il miglioramento delle tecnologie digitali nel settore pubblico*.

Come giustamente sottolineato da Aldo Agostinelli, soprattutto nel settore della PA si è reso necessario costruire nuove “autostrade” che garantiscano e sostengano lo sviluppo economico del paese.

A questo proposito è nata la **Strategia Cloud Italia**, annunciata dal ministro dell'Innovazione Vittorio Colao. *L'obiettivo è quello di eliminare gli oltre 11.000 data center sparsi in tutta Italia, facendo trasmettere i dati di almeno il 75% degli uffici pubblici italiani. Il piano sarà completato entro il 2025 e ad esso verranno destinati 1.9 miliardi dal PNRR.*

Come ogni cambiamento ambizioso, la Strategia Cloud Italia è associata ad una serie di opportunità, senza essere priva di rischi e dalla presenza di punti interrogativi ancora poco chiari. In questo paragrafo introduttivo, cercheremo di offrire una visione quanto più ampia delle opportunità, dei rischi e dei punti interrogativi associati.

Tipologie di Cloud

Infrastructure as Service (IaaS)

“Infrastruttura come Servizio” consiste nell’offrire accesso in forma on-demand risorse come rete, storage e server. Il cliente può così far girare le proprie piattaforme ed applicazioni direttamente sull’infrastruttura del provider.

Platform as a Service (PaaS)

“Piattaforma come Servizio” consiste in un modello di cloud dove il provider fornisce strumenti hardware e software da utilizzare in maniera per l’appunto remota. Tramite questo modello, tutti gli strumenti vengono eseguiti sulla piattaforma del provider.

Software as a Service (SaaS)

“Software come Servizio” consiste in un modello di licenza software in cui l’accesso al software stesso è fornito sulla base di un abbonamento, con il programma/servizio ospitato su server esterni invece che in-house. Solitamente si accede al SaaS tramite browser, con grande facilità di implementazione, aggiornamento e con benefici in termini di costo che lo rendono uno dei servizi più venduti sul mercato cloud.

2. LA CRONOLOGIA DEL CLOUD PER LA PUBBLICA AMMINISTRAZIONE

L'obiettivo del seguente paragrafo è, da una parte, quello di ripercorrere gli sviluppi di politiche e disposizioni in materia di **Cloud computing per la Pubblica Amministrazione**, dall'altra, di individuare le infrastrutture esistenti al momento in cui si scrive per analizzare, in seguito, la loro (possibile) dismissione o perpetuazione all'interno dell'attuale Strategia Cloud Italia.

2.1. Il Sistema Pubblico di Connettività e la gara SPC cloud lotto 1

Il Sistema Pubblico di Connettività (**SPC**) è una cornice nazionale di interoperabilità. L'SPC *"definisce le modalità preferenziali che i sistemi informativi delle pubbliche amministrazioni devono adottare per essere tra loro interoperabili"* (1).

È importante distinguere, all'interno del SPC, i ruoli dei due attori principalmente coinvolti: **Consip** e **AgID**.

Nel 2012, con la legge n°134, conversione con modificazione del decreto legge n. 83 del 2012 (cosiddetto "decreto sviluppo"), fu affidato a Consip il ruolo di centrale di committenza. Il compito di Consip era quello di gestire le gare d'appalto per la PA relativamente alle reti telematiche delle pubbliche amministrazioni, al sistema pubblico di connettività, alla rete internazionale della pubblica amministrazione.

1 AgID, Sistema Pubblico di Connettività <https://www.agid.gov.it/it/infrastrutture/sistema-pubblico-connettivita>

Mentre AgID, sempre nel rispetto di quanto prescritto dal D.L. n. 83/2012, convertito con la Legge n. 134/2012:

- detta indirizzi, regole tecniche e linee guida in materia di sicurezza informatica e di omogeneità dei linguaggi, delle procedure e degli standard in modo da assicurare la piena interoperabilità e cooperazione applicativa tra i sistemi informatici della pubblica amministrazione e tra questi e i sistemi dell'Unione europea;
- vigila sulla qualità dei servizi e sulla razionalizzazione della spesa in materia informatica, anche in collaborazione con Consip S.p.A. (oltre che con Sogei S.p.A.);
- svolge attività di progettazione e coordinamento delle iniziative strategiche e di preminente interesse nazionale per la più efficace erogazione di servizi in rete della pubblica amministrazione a cittadini e imprese (2).

Per il successo della strategia di diffusione del *cloud* nella PA, la stessa AGID, insieme a Consip, aveva predisposto un quadro di gare per la fornitura di servizi innovativi alle amministrazioni, nella quale si collocano sia la gara per i servizi di connettività SPC sia la gara, suddivisa in quattro lotti, per i servizi di Cloud computing, di gestione delle identità digitali e sicurezza applicativa, di realizzazione di portali e servizi on-line e di cooperazione applicativa. Questa iniziativa, tenutasi nel 2016, aveva l'obiettivo di rendere disponibili alle amministrazioni pubbliche italiane servizi innovativi di carattere abilitante per la realizzazione dell'Agenda Digitale Italiana, forniti secondo un modello di *Community cloud*.

In particolare, il community cloud realizzato da Tim, con la supervisione di Agid e Consip, mediante la gara Spc cloud lotto 1, ha rappresentato il primo tentativo di sperimentare un cloud riservato alla Pubblica amministrazione, coinvolgendo oltre mille amministrazioni centrali e locali. Alla base vi era la consapevolezza che far diventare efficiente e sicuro l'accesso ai dati, rendendo disponibili servizi di qualità, fosse essenziale per il sistema-Paese.

2 AgID, Connettività <https://www.agid.gov.it/it/infrastrutture/sistema-pubblico-connettivita/connettivita>

Secondo i dati dell'Osservatorio Cloud & ICT as a Service della School of Management del Politecnico di Milano, nonostante il 66% degli enti pubblici italiani utilizzava già nel 2015 modelli di cloud computing, la diffusione era fortemente frammentata, con strategie divergenti, spesso in assenza di un obiettivo definito (3). Considerando la situazione di elevata frammentazione e disomogeneità dei sistemi informativi delle PA, era necessario definire un percorso evolutivo che accompagnasse le PA stesse verso un utilizzo efficiente e flessibile delle tecnologie ICT al fine di garantire economie di scala e favorire l'erogazione di servizi più adeguati alle esigenze di cittadini ed imprese.

2.2. Il Piano Triennale per l'informatica nella Pubblica Amministrazione 2017-2019

Il Piano triennale per l'informatica nella Pubblica Amministrazione 2017-2019, redatto da AgID in accordo con la Strategia di crescita digitale italiana 2014 – 2020 (4), prevedeva, tra gli obiettivi strategici, la *"realizzazione di un ambiente cloud della PA, omogeneo dal punto di vista contrattuale e tecnologico, riqualificando le risorse interne alla PA già esistenti o facendo ricorso a risorse di soggetti esterni qualificati e un risparmio di spesa derivante dal consolidamento dei data center e migrazione dei servizi verso il cloud."* (5)

Le linee d'azione per raggiungere tali obiettivi risultano essere:

- L'individuazione di un insieme di infrastrutture fisiche esistenti di proprietà della PA elette a Poli strategici nazionali (**PSN**).
- La definizione di un percorso delle PA verso il modello cloud, anche attraverso le risorse rese disponibili dai Poli strategici nazionali e le risorse messe a disposizione tramite **SPC-Cloud**.
- La definizione di un processo di qualificazione dei PSN.
- La definizione di regole e procedure per la qualificazione di altri Cloud Service Provider (**CSP**).

3 <https://www.osservatori.net/it/ricerche/infografiche/cloud-per-la-pa-pronti-al-decollo>

4 Presidenza del Consiglio dei Ministri, Strategia per la crescita digitale 2014-2020, 3 marzo 2015
https://www.agid.gov.it/sites/default/files/repository_files/documentazione/strat_crescita_digit_3marzo_0.pdf

5 AgID, Piano triennale per l'informatica nella Pubblica amministrazione 2017-2019
https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2017-2019/doc/01_piano-triennale-per-informatica-nella-pa.html

Inoltre, tutte le Pubbliche amministrazioni proprietarie di infrastrutture fisiche avevano l'obbligo di effettuare un censimento del proprio patrimonio ICT effettuato da Agid. In base ai risultati del rilevamento, le infrastrutture fisiche, se non qualificabili come PSN, furono divise in due categorie:

- **Gruppo A** - Data center di qualità che non sono stati eletti a Polo strategico nazionale, oppure con carenze strutturali o organizzative considerate minori. Simili strutture continuavano ad operare ma non potevano essere effettuati investimenti per il loro ampliamento o evoluzione. Dovevano comunque garantire continuità dei servizi e disaster recovery, fino alla completa migrazione, avvalendosi dei servizi disponibili con il Contratto quadro SPC Cloud lotto 1 o messi a disposizione dai Poli strategici nazionali.
- **Gruppo B** - Data center che non garantivano i requisiti minimi di affidabilità e sicurezza dal punto di vista infrastrutturale e/o organizzativo, o non garantivano la continuità dei servizi. Queste infrastrutture dovevano essere rapidamente consolidate verso uno dei Poli strategici nazionali o verso il cloud tramite i servizi disponibili con il Contratto quadro SPC Cloud lotto 1. *Quest'ultima disposizione venne poi eliminata nel Piano Triennale 2019-2021 prevedendo la loro completa dismissione.*

2.3. Le circolari AgID n° 2 e n° 3 del 2018

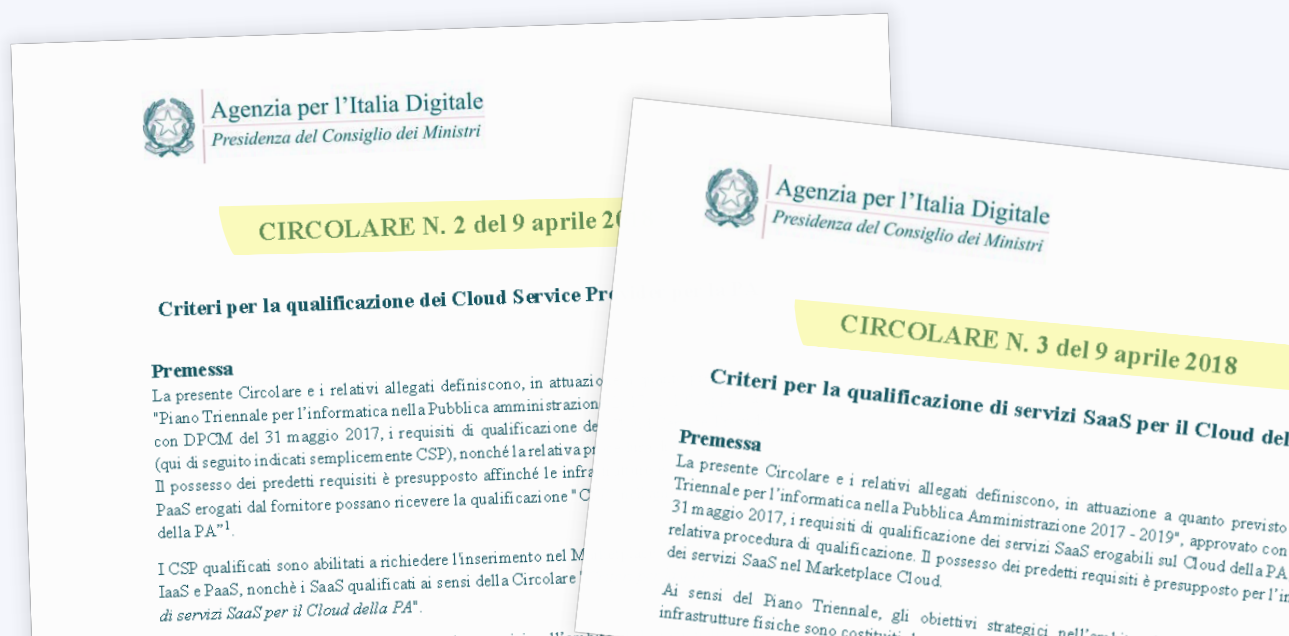
Come stabilito nel quarto punto delle linee d'azione del Piano triennale 2017-2019, AgiD aveva il compito di individuare dei criteri di qualificazione dei CSP. Ciò è stato reso possibile dalle circolari n° 2 e n° 3 del 2018, le quali definiscono procedure e requisiti per conseguire le qualificazioni di infrastrutture e servizi.

La prima, *"Criteri per la qualificazione dei Cloud Service Provider per la PA"* (6), definisce i requisiti per la qualificazione dei CSP e la relativa procedura di qualificazione. Il possesso dei predetti requisiti è presupposto per l'inserimento dell'infrastruttura Cloud all'interno del Registro Pubblico dei CSP qualificati e dei servizi IaaS e PaaS nel Cloud Marketplace.

La seconda, *"Criteri per la qualificazione di servizi SaaS per il Cloud della PA"* (7), definisce i requisiti per la qualificazione dei servizi SaaS erogabili sul cloud della PA e la relativa procedura di qualificazione. Il possesso dei predetti requisiti è presupposto per l'inserimento dei servizi SaaS nel Cloud Marketplace.

Le due circolari risultano essere di grande rilevanza, come si vedrà all'interno del sistema definito dal Piano Triennale 2019-2021.

-
- 6 AgID, CIRCOLARE N. 2 del 9 aprile 2018 https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/1811512344300_OCircolare+2-2018_Criteri+per+la+qualificazione+dei+Cloud+Service+Provider+per+la+PA.pdf
 - 7 AgID, CIRCOLARE N. 3 del 9 aprile 2018 https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/1811512372100_OCircolare+3-2018_Criteri+per+la+qualificazione+di+servizi+SaaS+per+il+Cloud+della+PA+%28002%29.pdf



2.4.

Il Piano Triennale per l'informatica nella Pubblica Amministrazione 2019 - 2021

Il **Piano triennale per l'informatica nella Pubblica amministrazione 2019-2021** ha individuato un modello ad hoc denominato "Cloud della PA". Questo si compone di tre elementi principali che caratterizzano il percorso di trasformazione:

1. "Il principio Cloud First secondo il quale le PA devono, in via prioritaria, adottare il paradigma cloud (in particolare i servizi SaaS) prima di qualsiasi altra opzione tecnologica per la definizione di nuovi progetti e per la progettazione dei nuovi servizi nell'ambito di nuove iniziative da avviare";
2. "Il modello Cloud della PA, il modello strategico che si compone di infrastrutture e servizi qualificati da AgID sulla base di un insieme di requisiti volti a garantire elevati standard di qualità per la PA";
3. "Il programma di abilitazione al cloud (cloud enablement program), l'insieme di attività, risorse, metodologie da mettere in campo per rendere le pubbliche amministrazioni capaci di migrare e mantenere in efficienza i propri servizi informatici (infrastrutture e applicazioni) all'interno del modello Cloud della PA" (8).

Il Piano ha sancito l'obbligo di approvvigionarsi dei soli servizi presenti sul *Cloud Marketplace* di AgID, la piattaforma che consente alle amministrazioni di consultare e confrontare le infrastrutture e i servizi cloud qualificati per la PA sulla base di parametri tecnici e funzionali. A tal fine, Consip, che dal 2012 gestiva i meccanismi di public procurement per la vendita dei servizi cloud alle PA, ha assicurato la conformità dei propri strumenti di acquisto (mercato elettronico, convenzioni, accordi quadro, contratti quadro, sistema dinamico di acquisto) alle circolari AgID 2 e 3 del 2018.

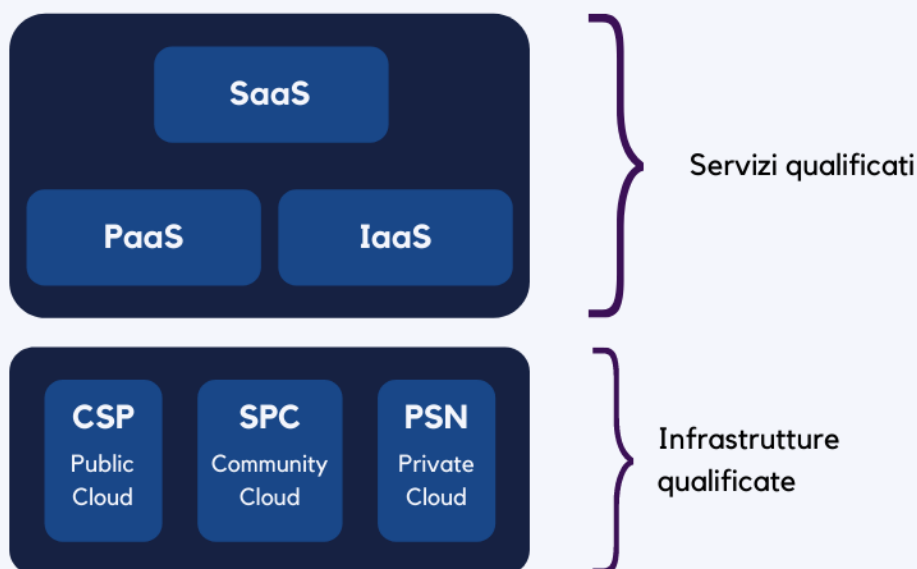
8 AgID, Piano triennale per l'informatica nella Pubblica amministrazione 2019-2021 https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2019-2021/03_infrastrutture.html#cloud-della-pa

I fornitori, indipendentemente dal fatto che fossero soggetti privati o loro stessi delle PA, devono utilizzare il Marketplace per sottoporre i propri servizi alla qualificazione di AgID. Qualificazione che poteva essere di tipo CSP (Cloud Service Provider) e/o SaaS. Nel dettaglio, la prima consente di erogare alle PA servizi di tipo IaaS e PaaS. Chi invece voleva erogare di tipo SaaS doveva indicare l'infrastruttura qualificata o i servizi qualificati su cui questi erano effettivamente basati. Anche nel caso in cui il fornitore volesse affidarsi a una propria infrastruttura cloud, questa doveva obbligatoriamente rientrare tra i CSP qualificati.

Perciò, i servizi cloud a disposizione della PA erano e sono erogati mediante le infrastrutture qualificate: i Cloud Service Provider (CSP) qualificati da AgID, i Poli Strategici Nazionali (PSN) e l'infrastruttura di Community Cloud realizzata dal Raggruppamento Temporaneo di Imprese (RTI) aggiudicatario del Contratto Quadro Consip SPC Cloud Lotto 1, fino al termine del contratto.

Tra l'altro, all'interno del Piano Triennale 2019-2021 è stato delineato il modello Cloud della PA, il quale contempla cloud di tipo pubblico, privato e community. La valutazione della tipologia di modello cloud da adottare è guidata principalmente dalla finalità del servizio all'utente e dalla natura di dati trattati. Il Piano prevede perciò un sistema fondato su 3 pilastri come esemplificato nella seguente figura.

CLOUD DELLA PA



2.5. L'articolo 35 del Decreto Legge semplificazioni del 2020

La tappa successiva in questo tentativo di ripercorrere le principali disposizioni in ambito cloud e amministrazione pubblica è costituita dal DL semplificazioni del 2020. In particolare, l'articolo 35 afferma che "la Presidenza del Consiglio dei ministri promuove lo sviluppo di un'infrastruttura ad alta affidabilità localizzata sul territorio nazionale per la razionalizzazione e il consolidamento dei Centri per l'elaborazione delle informazioni (CED) destinata a tutte le pubbliche amministrazioni." (9) Con il termine CED, o centro di elaborazione dati, si intende l'unità che ospita l'impianto informatico il cui compito è di coordinare e mantenere tutte le apparecchiature, i servizi di gestione dei dati, e l'intera infrastruttura IT a disposizione (10). Quindi il CED ha il compito di coordinare tutte le informazioni all'interno della pubblica amministrazione e i relativi flussi di diffusione e condivisione verso l'esterno.

L'articolo 35 prevede tre possibili destinazioni per la migrazione dei CED delle amministrazioni centrali e locali: infrastruttura promossa dalla Presidenza del Consiglio (PSN, rappresentato dal Polo Sogei per le amministrazioni centrali); infrastruttura propria già esistente e in possesso dei requisiti fissati da AgID o verso soluzioni di Cloud pubblico offerto mediante gara dai Cloud service provider.

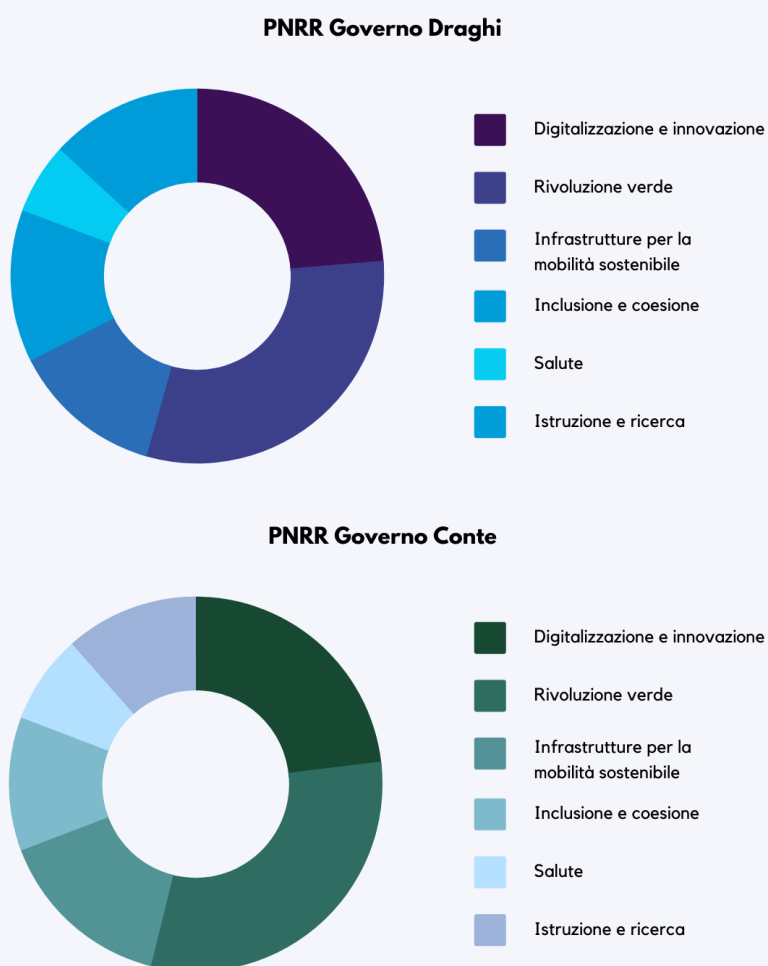
L'intento è di mettere in sicurezza le infrastrutture digitali delle pubbliche amministrazioni e al tempo stesso "migrare" i CED delle amministrazioni nel rispetto dei principi di efficienza, efficacia ed economicità dell'azione amministrativa.

9 DECRETO-LEGGE 16 luglio 2020, n. 76 <https://www.gazzettaufficiale.it/eli/id/2020/07/16/20G00096/sg>

10 <https://www.bucap.it/news/approfondimenti-tematici/continuita-operativa/ced-cosa-vuol-dire.htm>

2.6. La strategia per il cloud nazionale del Governo Conte II

Infine, l'ultima tappa normativa, che però non è mai stata attuata, prima della Strategia Cloud Italia, fu presentata dal Ministro per l'Innovazione Tecnologica e la Digitalizzazione Paola Pisano all'interno della bozza di PNRR del governo Conte Bis sottoposta al Parlamento il 15 gennaio 2021. Il grafico che segue riporta un confronto sulla percentuale di ripartizione dei fondi stimati dal Recovery and Resilience Facility, mostra come le percentuali dei due PNRR destinate al settore "Digitalizzazione e innovazione" sono rimaste invariate. Si è passati dal prevedere il 21,6% delle risorse del Recovery plan sotto il Governo Conte II al destinarne il 22% con il PNRR del governo Draghi.



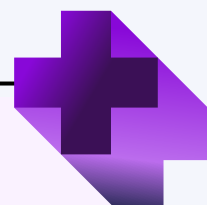
NEL GRAFICO: Suddivisione percentuale delle risorse del Recovery and Resilience Facility nel PNRR del governo Conte bis e nel PNRR del governo Draghi

Fonte: <https://pagellapolitica.it/blog/show/1054/che-cos%C3%A8-cambiato-nel-piano-nazionale-di-ripresa-e-resilienza>

Sebbene le due strategie risultino essere simili dal punto di vista quantitativo, esse sono qualitativamente diverse. Di fatto, la strategia del Ministro Pisano prevedeva la creazione di un cloud nazionale pubblico, attraverso un partenariato pubblico-privato e di un PSN, in conformità con l'articolo 35 del DL Semplificazioni 2020. Inoltre, prevedeva una forte sinergia con il progetto europeo Gaia-X e la realizzazione di un Cloud Enablement Program per favorire l'aggregazione e la migrazione delle PA centrali e locali verso soluzioni cloud e fornire alle stesse PA procedure, metodologie e strumenti di supporto utili a questa transizione (11).

Nonostante tale strategia non sia stata mai implementata, viene criticata per due ragioni: da una lato, per la mancanza di un criterio di classificazione dei dati da destinare ai due tipi di cloud previsti, dall'altro per la scelta del partenariato pubblico-privato per la creazione del cloud nazionale.

11 Piano Nazionale di Ripresa e Resilienza, 12 gennaio 2021
https://www.governo.it/sites/new.governo.it/files/PNRR_2021_0.pdf



GAIA-X: luci ed ombre del progetto di un cloud federato europeo

Nel giugno del 2020 Francia e Germania, ancora una volta attori trainanti delle politiche industriali europee, hanno deciso di unire le forze nella costituzione di Gaia-X, sostanzialmente una “piattaforma” per la creazione di un cloud federato europeo. L'associazione però non ha intenzione di diventare un provider, bensì di coordinare in maniera ancora non del tutto definita l'architettura dell'infrastruttura e dei servizi cloud europei. L'importanza di questo progetto è stata poi suggellata dallo Stato dell'Unione pronunciato da Ursula Von der Leyen proprio nel settembre dello stesso anno, a sottolineare le concrete intenzioni della Commissione nello sfidare i provider americani e cinesi.

Molti player europei, principalmente rappresentanti Germania, Francia, Italia, Belgio e Olanda, hanno preso parte al progetto. Eppure, a 16 mesi di distanza dalla sua creazione, l'agenda cloud europea sembra relativamente ferma e confusa, con Gaia-X attualmente maggiormente impegnata a risolvere dispute interne piuttosto che altro.

Secondo quanto riportato da Politico, sembra infatti che molti membri dell'associazione siano piuttosto scontenti delle intricate procedure burocratiche e del tentativo da parte dei player francesi di "prendere il controllo" della federazione. Proprio Macron ed il ministro del digitale francese Cédric O hanno sottolineato più volte l'estremo ritardo dell'Europa nel portare avanti il proprio progetto di cloud sovrano. Anche l'attuale CEO di Gaia-x, l'italiano Francesco Bonfiglio ha riconosciuto le difficoltà e le frustrazioni attualmente presenti nell'organizzazione, rimanendo però convinto della capacità del progetto di portare a termine i suoi obiettivi.

Altri dubbi sono invece sorti su Gaia-x quando ad Aprile 2021, Google, Amazon, Palantir, Huawei e Alibaba hanno preso anch'essi parte al progetto come membri a pieno titolo. Ciò ha quindi suscitato forti perplessità sulla capacità del progetto di rimanere autonomo, quando player americani e cinesi sono ora coinvolti nella stesura delle future regole per un cloud "sovrano". Sembra infatti che l'egemonia di questi player non europei sia imprescindibile in quasi ogni ramificazione del settore cloud, come confermato dalle partnership italiane con provider americani e dall'accordo tra Google con Orange in Francia e Deutsche Telekom in Germania.

Al di là delle numerose problematiche, sembra finalmente che Gaia-x sia pronta a lanciare la sua prima concreta iniziativa durante il Gaia-X Summit che si terrà il 18 e 19 Novembre a Milano. A quanto pare verrà inaugurato il primo sistema di certificazione cloud europeo, che segnerà il livello di sicurezza dei servizi cloud su 3 gradi. Il livello più elevato consisterà in un servizio cloud con dei dati completamente conservati ed operati su server fisicamente localizzati in Europa. Inoltre, un provider di livello 3 dovrà anche garantire agli utenti la possibilità di trasferire i propri dati ad un provider differente. In un mercato sempre più orientato a prodotti cloud sicuri e flessibili, il sistema ideato da Gaia-X potrebbe eventualmente avere un decisivo impatto sul mercato interno europeo, specialmente in ottica di cloud governativi e finanziate dai vari piani di resilienza degli stati membri.



Abbiamo quindi ripercorso i diversi approcci al cloud che si sono succeduti negli anni. Cercheremo ora di evidenziare, attraverso un sistema di similitudini e confronti, quale potrà essere il loro ruolo nella nuova Strategia Cloud Italia, che verrà dettagliata nel successivo paragrafo.

3. STRATEGIA CLOUD ITALIA

La Strategia Cloud Italia è il risultato di un processo normativo iniziato nel 2016. Ripercorrere queste tappe è di fondamentale importanza per comprendere al meglio lo stato dell'arte infrastrutturale del Paese e, di conseguenza, ponderare l'economicità dell'approccio messo in atto dall'attuale governo.

Il 7 settembre 2021 Vittorio Colao, Ministro per l'innovazione tecnologica e la transizione digitale, insieme a Franco Gabrielli, Sottosegretario di Stato delegato alla Sicurezza, Roberto Baldoni, Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, e Paolo De Rosa, Chief Technology Officer del Dipartimento per la Trasformazione digitale, ha presentato la "Strategia Cloud Italia". Questa si inserisce nel quadro dei finanziamenti previsti dal Piano Nazionale di Ripresa e Resilienza (PNRR) per la digitalizzazione che ammontano a un totale di 9,75 miliardi di euro. Nello specifico, il supporto finanziario alla base di tale strategia è pari a 1 miliardo (12).

L'obiettivo principale è quello di trasferire i dati della Pubblica Amministrazione, attualmente conservati in 11mila data center, sul Cloud nazionale al fine di aumentarne il livello di sicurezza.



3.1. Il processo di classificazione dei dati

La strategia prevede di classificare i dati in tre categorie: dati ordinari, strategici e critici. Le tre categorie di dati individuate corrispondono all'entità del danno che verrebbe causato da una loro manomissione. Perciò, seguendo questa logica, i dati ordinari sono quei dati la cui violazione non pregiudicherebbe l'integrità statale; all'interno di questa categoria ricadrebbero tutti quei dati disponibili sui portali amministrativi istituzionali. Al contrario, un potenziale cyberattacco a dati critici, come per esempio quelli sanitari, potrebbe avere conseguenze negative sul benessere economico e sociale del Paese. Infine, la manomissione di dati strategici, dati provenienti dal Perimetro di Sicurezza Nazionale Cibernetico (PSNC), cioè l'insieme di reti, sistemi e servizi informatici da cui dipende l'esercizio di una funzione essenziale dello Stato, potrebbe compromettere la sicurezza nazionale (13).

3.2. Il processo di qualificazione dei servizi cloud

Il processo di categorizzazione verrà eseguito tramite specifici questionari sottoposti alle singole amministrazioni e, a seconda della tipologia di dato, questo verrà conservato in un cloud qualificato. Tale processo è fondamentale per una migrazione al cloud uniforme e sistemica. La qualificazione dei servizi Cloud è elemento essenziale e mira a comprendere come viene effettuata la gestione operativa dei servizi. In particolare, vi sono tre categorie di requisiti per qualificare il cloud, in base al livello di controllo che si esercita sui dati:

- Gestione operativa dei servizi Cloud, in particolare gli standard tecnico-organizzativi e le misure di controllo sui dati.
- Requisiti di sicurezza e in particolare le modalità di gestione delle chiavi di cifratura.
- Clausole contrattuali con riferimento all'erogazione del servizio e alla sua rendicontazione.

13 Dipartimento per la Trasformazione Digitale, Strategia Cloud Italia Documento sintetico di indirizzo strategico per l'implementazione e il controllo del Cloud della PA <https://assets.innovazione.gov.it/1634299755-strategiacloudit.pdf>

Alla luce di ciò la Strategia Cloud Italia esclude l'utilizzo del Cloud pubblico non qualificato. In questo caso, il CSP non è qualificato rispetto alla normativa UE e non rispetta i requisiti tecnico-organizzativi. Perciò, i rischi posti dall'approvvigionamento da fornitori di paesi non europei, come si vedrà nella sezione 6 in modo più approfondito, vanno da possibili modifiche unilaterali delle condizioni dei servizi forniti, fino a rischi sistemici dovuti alla normativa in essere in tali paesi che garantiscono l'accesso ai dati presenti sui loro sistemi.

I tre requisiti sopraelencati delineano perciò quattro livelli di capacità di controllo dei dati e di conseguenza quattro tipologie di cloud:

- Cloud pubblico qualificato: rispetta il quadro legislativo europeo (GDPR e NIS). Tale servizio consente la localizzazione dei dati in UE e il rispetto di requisiti di sicurezza tecnico-organizzativi sulla base di sistemi di cifratura gestiti dal fornitore. Esso garantisce la gestione delle chiavi di accesso ai dati in Italia da parte della PA.
- Cloud pubblico con controllo on-premise: anche detto cloud pubblico con controllo on-premise dei meccanismi di sicurezza. Consente un controllo maggiore sui dati e servizi e sulle infrastrutture tecnologiche. Questo è possibile grazie alla possibilità di accesso al servizio attraverso software installati fisicamente nei computer (on-premise, in sede).
- Cloud privato/ibrido(IT): 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:
 - Cloud privato/ibrido su licenza: in questo caso i fornitori con tecnologia di cloud pubblico sono in grado di lavorare all'interno delle infrastrutture delle PA o di un loro fornitore. Oltre a garantire flessibilità e controllo sui dati, vi è anche controllo su hardware e software.
 - Cloud privato qualificato: utilizza delle tecnologie industry standard, ma l'intera filiera è fornita dal fornitore e consente il massimo controllo sui dati. I requisiti di sicurezza sono garantiti dalla crittografia nazionale con controllo delle chiavi in Italia.

Questa classificazione permette di adottare soluzioni specifiche per le diverse PA e di conservare i diversi tipi di dati all'interno di servizi Cloud più adatti. Perciò dati ordinari potranno essere detenuti in un cloud di tipo pubblico qualificato o pubblico criptato. I dati critici potranno invece essere conservati in cloud di tipo pubblico criptato, privato/ibrido "su licenza" o privato e infine, dati e servizi strategici potranno essere detenuti su un cloud di tipo privato/ibrido "su licenza" o privato.

3.3. Il Polo Strategico Nazionale

Altro pilastro fondamentale della Strategia è la costituzione del Polo Strategico Nazionale, ossia di un'infrastruttura informatica presente in vari punti del territorio nazionale. Questo dovrebbe essere costituito da quattro data center collocati in almeno due regioni, l'obiettivo è quello di garantire adeguati livelli di continuità operativa e tolleranza ai guasti. In accordo alla classificazione fornita precedentemente, il PSN offrirà servizi di Cloud Pubblico Criptato, 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", il Cloud Privato Qualificato. Inoltre, il PSN offrirà supporto alle amministrazioni centrali e alle principali amministrazioni locali come, ad esempio, Regioni, ASL e città metropolitane.

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, il rispetto dei requisiti in materia di sicurezza (requisiti by-design), ad esempio PSNC e NIS, e di abilitare la migrazione verso tipologie di servizi Cloud IaaS (Infrastructure as a Service) e PaaS (Platform as a Service).

L'obiettivo per i prossimi cinque anni è quello di migrare i dataset e le applicazioni di una parte consistente delle PA locali verso un'infrastruttura cloud sicura, lasciando a ciascuna amministrazione la libertà di scegliere all'interno di un insieme di cloud provider pubblici certificati. Qualora ci fossero situazioni in cui la sensibilità dei dati è tale da non ritenere accettabile una soluzione di cloud pubblico, l'amministrazione potrebbe scegliere di utilizzare invece il PSN ibrido o privato.

3.4. Il futuro delle infrastrutture esistenti

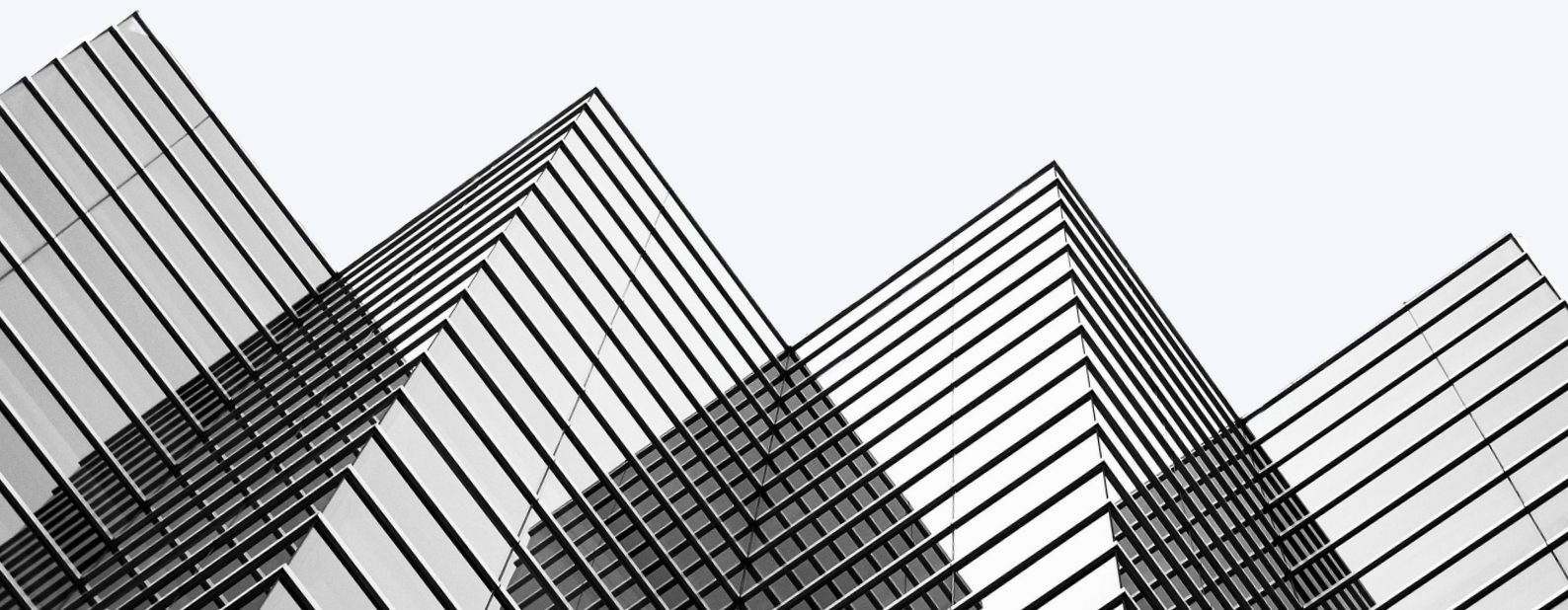
Alla luce dell'analisi svolta finora ci si può chiedere quali delle infrastrutture esistenti possano essere perpetuate e quindi utilizzate per sviluppare la Strategia Cloud Italia e quali verranno invece dismesse. Di fatto, è presente in Italia un patrimonio di infrastrutture e servizi che può essere opportunamente integrato e valorizzato al fine di economizzare la migrazione al cloud.

Per quanto riguarda cloud e datacenter pubblici, la razionalizzazione promossa da AgID ha dato un primo boost ad una migrazione sicura al cloud, come previsto dal Piano Triennale per l'informatica nella Pubblica amministrazione 2019-2021. Il percorso prevede la progressiva dismissione dei data center obsoleti e inefficienti, con l'obiettivo di ridurre i costi di gestione delle infrastrutture IT in favore di una migrazione verso il Cloud della PA.

Il censimento è stato condotto da AgID su quasi mille amministrazioni per un totale di 1252 data center censiti con l'obiettivo di rilevare lo stato delle infrastrutture IT della PA.

Dei 1252 data center censiti:

- 35 sono risultati candidabili all'utilizzo da parte del Polo strategico nazionale, grazie all'affidabilità delle infrastrutture.
- 27 sono stati classificati nel gruppo A, ossia data center di media qualità ma non candidabili a PSN.
- I restanti 1190 sono stati classificati nel gruppo B, cioè quei data center privi di requisiti minimi di affidabilità e sicurezza e incapaci di garantire la continuità del servizio. Il loro destino è la progressiva dismissione.



Per quanto riguarda il PSN, infrastruttura al centro della strategia di digitalizzazione della PA fin dal 2017, anch'esso pone vari punti aperti.

Operativamente, quel che sappiamo oggi dalle fonti ufficiali è che il PSN sarà distribuito geograficamente in due diverse regioni e articolato in quattro data center. La gestione operativa del PSN sarà affidata a un operatore economico, selezionato attraverso l'avvio di un partenariato pubblico/privato (PPP) ad iniziativa di un soggetto proponente. Al riguardo, le cordate che hanno presentato ad oggi la loro proposta al ministero sono due: la prima è costituita da Tim, Leonardo, Sogei e Cdp, la seconda da Al maviva e Aruba.

Per esempio, ci si potrebbe chiedere se e in che misura verrà integrato il già esistente Polo Sogei. Come ricorda Andrea Quacivi, amministratore delegato di Sogei, in un'intervista al Sole24Ore, "Sogei è Polo strategico nazionale per legge. Il Decreto legislativo 179/2016 assegna a Sogei la creazione di uno dei Psn descritti nel Piano Triennale appartenenti al Cloud della Pa" (14). Inoltre, Sogei è una delle società pubbliche che partecipano al bando per la creazione del PSN insieme a Tim, Leonardo e Cassa depositi e prestiti. Questa cordata sembra per di più essere la più accreditata a vincere la gara d'appalto in atto.

Come si è già visto, dal 2019 la Pubblica Amministrazione italiana può acquistare solo servizi Cloud dai CSP qualificati e pubblicati sul "Catalogo dei servizi Cloud qualificati per la PA" realizzato da AgID. Si tratta di una lista di società, a prevalenza di multinazionali che dominano i mercati mondiali del Cloud (Microsoft, Google e Amazon).

Ci si chiede dunque quale sarà il ruolo del Marketplace all'interno della Strategia Cloud Italia. Ci si potrà basare su questo catalogo secondo i criteri già utilizzati da AgID per qualificare i CSP? Infine, il CSP Cloud Lotto 1 sarebbe dovuto essere dismesso nel 2021 ma è stato prorogato fino a dicembre 2022. Se ritenuto necessario, si potrebbe pensare ad un'ulteriore proroga e un suo potenziale inserimento nella strategia del ministro Colao.

14 Gianni Dragoni, "Sogei polo strategico per la PA digitale" - Intervista a Andrea Quacivi, il Sole 24 ore, 28 marzo 2019 <https://www.sogei.it/it/sogei-homepage/azienda/sala-stampa/Articolieinterviste/articoli-e-interviste-2019/sogei-polo-strategico-per-la-pa-digitale----intervista-a-andrea.html>

4. UN CLOUD NAZIONALE ITALIANO: OPPORTUNITÀ, RISCHI E PUNTI INTERROGATIVI

4.1. Quali opportunità?

Quello appena descritto rappresenta senza dubbio un cambiamento cruciale per la digitalizzazione di tutto l'apparato della PA. Le principali opportunità che questo progetto presenta sono state riassunte in tre filoni principali:



Fonte: <https://aliautonomie.it/wp-content/uploads/2021/09/Strategia-Cloud-Italia-2021ita.pdf>

1

L'opportunità di assicurare l'autonomia tecnologica del Paese

Allo stato attuale, le quote di mercato dei servizi, delle piattaforme e soprattutto delle infrastrutture Cloud detenute dalle aziende europee sono molto ridotte rispetto a quelle delle aziende extra-UE. Questo si traduce in una debolezza contrattuale, che rende i paesi europei soggetti al rischio di modifiche unilaterali delle condizioni di servizio da parte di provider esteri. Per questo, il raggiungimento di un'autonomia tecnologica avrebbe notevoli ricadute sull'economia dei dati e non solo.

2

L'opportunità di garantire il controllo sui dati

La gestione dei servizi Cloud da parte di fornitori di paesi extra UE presenta attualmente un rischio aggiuntivo dovuto alla normativa in essere in tali paesi, che può portare alla richiesta unilaterale al fornitore dei servizi Cloud di fornire l'accesso ai dati. La Strategia Cloud Italia servirà ad evitare che un Paese Terzo possa accedere a dati italiani strategici, sarà necessario e a dettagliare quali sono i requisiti di sicurezza necessari per la gestione di dati sensibili.

3

L'opportunità di aumentare la resilienza dei servizi digitali

Questo ultimo punto è inteso come processo di qualificazione dei fornitori di Cloud pubblico e dei loro servizi. In particolar modo, ci si riferisce alla standardizzazione, armonizzazione ed interoperabilità dei servizi Cloud. In quest'ottica, è stato avviato il progetto GAIA-X, che mira a costituire un ecosistema digitale aperto e resiliente mediante la federazione di servizi Cloud, basati su standard comuni a garanzia di trasparenza e interoperabilità, in grado di collegare creando un ecosistema omogeneo.

4.2. Rischi

Come ogni medaglia ha un dritto e un rovescio, la Strategia Cloud Italia, ricca di opportunità, non è priva di rischi. Il tema della **Cyber Security** svetta per interesse e rilievo: per quanto più sicuro del mix di tecnologie e sistemi attualmente in uso, il cloud non è da considerarsi inespugnabile.

Primo fra tutti, perché la componente tecnologica andrà costantemente ad interfacciarsi con una importante componente umana. Un'opera così radicale di digitalizzazione sarà costretta a confrontarsi con l'eterogeneità della PA e del suo personale. Come spesso ribadito, *l'anello debole di qualsiasi catena di sicurezza è rappresentato dagli esseri umani*. Alcune pratiche, tra cui quella social engineering, cercano di sfruttare questo anello debole per spingere le persone a rivelare determinate informazioni o consentire l'accesso ad un sistema informato.

Tra le varie tecniche utilizzate esistono:

Baiting

(offrire qualcosa al fine di consentire il download di un file dannoso)

Phishing

(una mail realizzata appositamente per favorire l'inserimento di informazioni personali)

Scareware

(spingere l'utente a credere che il proprio computer sia infetto per poi offrire una soluzione con cui infettarlo veramente)

Pretexting

(impersonare qualcuno per ottenere l'accesso a dati privilegiati)

Quest'ultima riassume bene quello che è accaduto tra fine luglio e inizio agosto, quando un *ransomware* ha colpito il centro elaborazione dati (CED) della regione Lazio attraverso le credenziali VPN indebitamente sottratte a una dipendente di Frosinone. A migrazione completata, la potenzialità del ripetersi eventi simili potrebbe moltiplicarsi in modo esponenziale.

Una seconda e importante sfida sarà quella della messa in sicurezza dei nodi di accesso, distribuiti nei tantissimi comuni italiani e proposti al collegamento col cloud di stato. Dal punto di vista tecnico, gli *endpoint* rappresentano infatti potenziali punti di entrata per le minacce informatiche. **Risulta perciò indispensabile provvedere all'adeguata protezione di ogni anello della catena di rete**, a partire da questi che sono i più deboli.

Terzo, sarà necessario affrontare la questione di possibili *insider*, sia colposi che dolosi. Se nel primo caso si tratterebbe di esposizione di dati sensibili per un errore inconsapevole, nel secondo caso l'introduzione di un cloud nazionale potrebbe essere seguita da una strategia di reclutamento attivo di possibili insider.



WannaCry ransomware
Nota di ricatto di un sistema infettato
Maggio 2017 - Cyberattacco mondiale

Ne consegue che per avere successo il cloud di stato dovrà garantire un framework dinamico, tale da scongiurare di volta in volta nuove e pressanti minacce.

In particolare, sarà interessante valutare come verranno effettivamente declinati in questo contesto i *tre livelli di sicurezza*:

- quella **predittiva** (per comprendere a priori le minacce),
- **preventiva** (che si identifica con l'analisi del rischio attraverso attività di analisi specifiche del rischio intese nel senso più ampio del termine)
- e **proattiva** (intesa soprattutto come la capacità di reazione ad eventuali attacchi).

In relazione a quest'ultima categoria, lo stesso Carta – presidente di Leonardo – aveva puntualizzato che: *“sarebbe importante prevedere un meccanismo di protezione del dato tramite un **algoritmo di cifratura esclusivamente "nazionale"** certificato dall'Autorità nazionale per la sicurezza che gestisce e distribuisce le necessarie chiavi di protezione. Anche così si contribuisce a rafforzare il perimetro di difesa nazionale da possibili esfiltrazioni”*.

4.3. Punti interrogativi

Il tema inerente il supporto delle amministrazioni si lega a quello delle competenze. Nel ricordare che molti dipendenti pubblici sono andati in pensione, portando con sé la memoria storica dei sistemi in funzione, Antonio Cisternino ha evidenziato come *“le PA soffrono molto l’assenza di competenze in un panorama sempre più complesso e parcellizzato, dove solo per capire un modello di cloud o decodificare alcune linee guida servono competenze in parte o del tutto assenti”*.

Non si può che essere d’accordo che le (poche) nuove assunzioni soffrono di un problema centrale: **come attrarre competenze**. Se la struttura salariale del lavoro pubblico non è in grado di attrarre adeguate professionalità, attratte da un mercato ICT in grado di remunerare meglio del settore pubblico, c’è da chiedersi con quali risorse si dovranno gestire i fornitori a cui si dovrà necessariamente far ricorso per la migrazione dei servizi esistenti e la realizzazione dei nuovi.

Diventa cruciale mettere al centro dell’attenzione il tema della **formazione**, altrimenti è difficile immaginare chi possa davvero supportare la transizione di oltre 20.000 enti. Troppe amministrazioni, specialmente a livello locale, non hanno ancora individuato il *Responsabile per la Transizione Digitale*, oppure hanno portato avanti una nomina da adempimento senza, però, una piena consapevolezza dell’importanza del ruolo nell’attuazione del piano. La formazione degli RTD e del personale del suo ufficio è e resta un tema centrale per sostenere un reale cambiamento.

5. **QUALE CLOUD PER L'AMMINISTRAZIONE PUBBLICA?**

Investire in tecnologie ICT per modernizzare le infrastrutture statali è una tendenza crescente che deve essere accompagnata da una precisa analisi del contesto e delle necessità, alle quali una particolare tecnologia deve rispondere.

La migrazione dei dati della Pubblica Amministrazione, macchina burocratica dello Stato, sulla nuvola cloud deve essere ponderata attraverso due tipi di analisi. La prima, di tipo tecnico-infrastrutturale, la seconda di tipo socio-economico che abbia in considerazione, tra le altre cose, le competenze richieste e i costi di un simile investimento.

Come si è visto l'approccio dell'attuale governo è fortemente misto, prevedendo soluzioni cloud (pubblico, privato o ibrido) in base al grado di confidenzialità dei dati trattati. Nonostante, dal punto di vista operativo, tale scelta comporti alcuni problemi, risulta essere una strategia fortemente coerente poiché i tre tipi di cloud rispondono ad esigenze diverse. Allo stesso tempo gli enti della Pubblica Amministrazione trattano dati di natura completamente diversa l'uno dall'altro e, di conseguenza, richiedono gradi di confidenzialità e sicurezza diversi.

Solo per citare uno dei problemi operativi appena accennati e posto dal cloud pubblico, si parla di lock-in verso il fornitore quando il cliente dipende dal punto di vista tecnologico da alcuni servizi esclusivi erogati dal fornitore. Lo stesso Piano triennale 2019-2021 stabilisce tra i suoi obiettivi la necessità di ridurre il rischio di dipendenza esclusiva dal fornitore (vendor lock-in) senza però fornire alcun tipo di raccomandazione per impedire che ciò avvenga. Può accadere che i CSP impongano dei blocchi all'uscita dal proprio servizio con l'intento di contenere all'interno della propria offerta i clienti ed evitare migrazioni verso i competitor. Per questo motivo il processo di transizione da un CSP ad un altro diventa complesso, se non impossibile. Questo comporta non pochi problemi. Uno tra essi è che se il CSP decide di aumentare il prezzo del servizio l'ente a cui esso è erogato si trova in una condizione da cui è difficile togliersi. Perciò, mitigare questo rischio significa analizzare con estrema attenzione le clausole dei contratti cloud e negoziare con i provider formule che privilegino interoperabilità, flessibilità e libertà di scelta non solo sul piano del servizio core, ma anche rispetto alle opzioni e alla personalizzazione.

5.1. AWS GovCloud (US) e il caso statunitense

Com'è stato ribadito più volte, la scelta del tipo cloud da adottare avviene in base alle necessità del soggetto in questione. Per fare un esempio, il governo federale statunitense ha optato per un cloud privato fornito da Amazon Web Services (AWS).



Nel febbraio 2011, il primo CIO federale del governo statunitense, Vivek Kundra, ha annunciato la strategia del cloud first (15). La politica è stata presentata come un aspetto cruciale degli sforzi di riforma del governo per aumentare l'efficienza operativa tagliando gli sprechi e aiutare le agenzie governative a fornire servizi in modo più snello e veloce.

Le regioni AWS GovCloud sono regioni cloud isolate di Amazon Web Services, il cui scopo è quello di gestire i carichi di lavoro con legami diretti o indiretti con servizi del governo degli Stati Uniti. Tutti i clienti che usano GovCloud devono essere organizzazioni governative o altre entità private approvate in settori legati al governo come l'aerospaziale, le forze dell'ordine e la sanità (16).

15 Vivek Kundra, Federal cloud computing strategy, 8 febbraio 2011

https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud--strategy.pdf

16 AWS, AWS GovCloud (US) <https://aws.amazon.com/it/govcloud-us/?whats-new-ess.sort-by=item.additionalFields.postDateTime&whats-new-ess.sort-order=desc>

Attualmente ci sono due regioni di GovCloud, US-West e US-East. Le regioni sono fisicamente situate negli Stati Uniti e sono progettate per consentire alle agenzie governative e ai loro partner di spostare i carichi di lavoro sensibili nel cloud rispettando allo stesso tempo specifici requisiti normativi e di conformità. Tali soluzioni cloud risultano essere estremamente sicure perché conformi alla Federal Risk and Management Program (FedRAMP), alla High Department of Defense Security Requirements Guide (DoD SRG) alla politica di sicurezza dei sistemi informativi della giustizia penale (CJIS) del Dipartimento di giustizia, alle normative sul traffico internazionale di armi (ITAR) e ad altri regimi di conformità. (17)

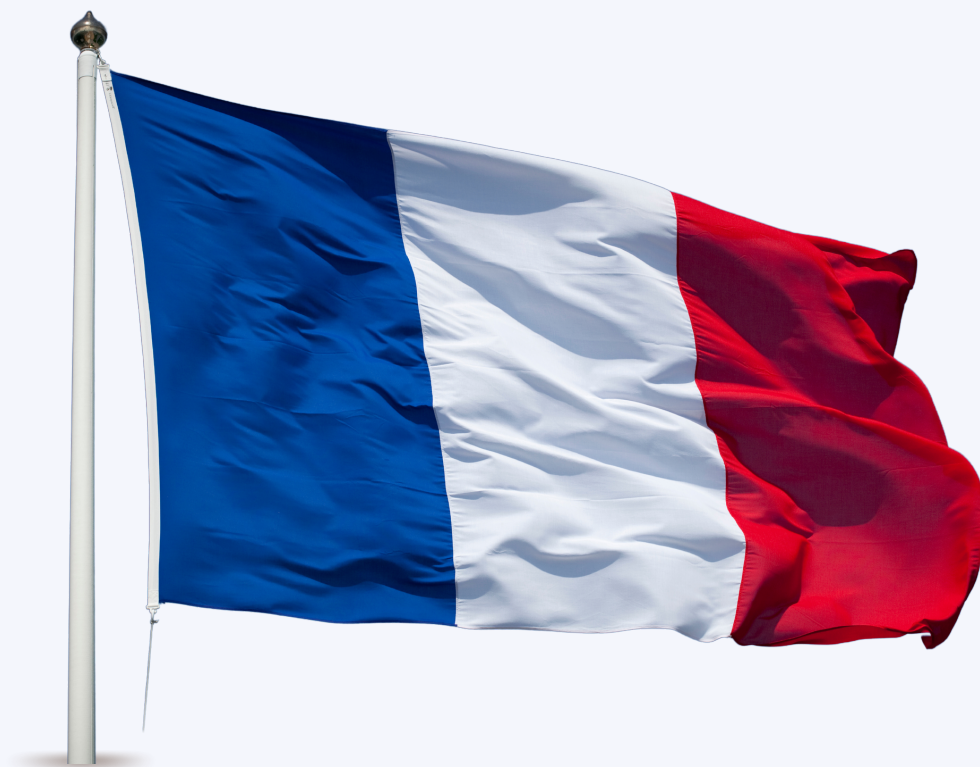
AWS GovCloud (US) tratta una grande varietà di dati partendo da quelle che vengono definite informazioni non classificate controllate (CUI), ossia quelle prive di classifica di segretezza, ma ritenute meritevoli di protezione, ad esempio attraverso la limitazione dell'accesso alle sole persone che hanno necessità di trattarle per motivi attinenti al loro impiego, incarico o professione, fino a informazioni personalmente identificabili (PII) passando per le cartelle cliniche sensibili dei pazienti, i dati finanziari, quelli delle forze dell'ordine e i dati sulle esportazioni (18).

Una simile scelta deriva perciò dalla consapevolezza che i dati del governo sono dati particolarmente vulnerabili, che richiedono alti livelli di sicurezza e di riservatezza. In particolare, l'infrastruttura sicura di AWS ha aiutato le agenzie federali a espandere il cloud computing e a inserire dati governativi sensibili nel cloud, rispettando i rigorosi requisiti di sicurezza degli standard federali.

17 MITRE, AWS GovCloud Resource and Cost Analysis, gennaio 2020 <https://apps.dtic.mil/sti/pdfs/AD1114483.pdf>

18 Cloud.Gov, Infrastructure under cloud.gov <https://cloud.gov/docs/computingtechnology/iaas/>

6. STRATEGIA FRANCESE



La migrazione al *cloud* porta alla luce tre grandi sfide: la **trasformazione delle aziende e amministrazioni**, la **sovranità digitale** e la **competitività economica**. Tuttavia, la nuvola presenta dei rischi per l'integrità dei dati, sia per ragioni tecniche, con l'aumento degli attacchi informatici, sia per ragioni legali, con la minaccia di legislazioni extraterritoriali che diano agli stati stranieri la possibilità di accedere ai dati di cittadini, amministrazioni e imprese.

Un modello che siamo andati a studiare in quest'ottica, è quello francese, il quale, per rispondere alle sfide prima citate, prevede una strategia basata su tre pilastri (19):

1. L'etichetta *Trusted Cloud (cloud de confiance)*, che permetterà alle aziende e alle amministrazioni francesi di beneficiare dei migliori servizi offerti dal cloud garantendo una maggiore protezione dei loro dati.
2. La politica "*Cloud al centro*" dell'amministrazione per accelerare la trasformazione digitale del servizio pubblico.
3. Una strategia industriale, parte del programma *France Relance*, che permetterà di stabilire la sovranità francese ed europea, accompagnando la costruzione di nuovi strumenti cloud.

19 Gouvernement français, Stratégie nationale pour le cloud, France Relance, 17 maggio 2021
<https://www.numerique.gouv.fr/uploads/Strategie-nationale-pour-le-cloud.pdf>

Alla base dell'efficacia della strategia francese vi è la consapevolezza che **il massimo livello di protezione dei dati deve operare sia a livello tecnico che giuridico**. Mentre le caratteristiche tecniche permettono di lottare contro i rischi di cyber attacchi, il livello giuridico deve proteggere gli stessi dati contro i rischi di applicazione di leggi extraterritoriali non conformi ai valori europei. Sebbene implicito, il riferimento è a due normative americane: **il Cloud Act** e **il Fisa 702**. Inoltre, i servizi Cloud più efficienti sono erogati da aziende straniere, in particolare americane. È a questo doppio problema che il marchio Trusted Cloud tenta di rispondere.

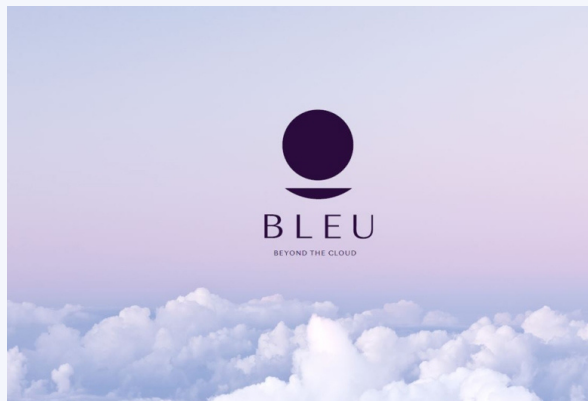
L'etichetta "**Trusted Cloud**", che si basa sul visto SecNumCloud rilasciato dall'*Agenzia Nazionale per la Sicurezza dei sistemi informatici* (ANSSI), sarà concessa ai fornitori di servizi. Dovrebbe quindi offrire un doppio livello di sicurezza - giuridico e tecnico - alle imprese e alle amministrazioni francesi.

Di fatto, l'etichetta permetterà alle aziende americane di commercializzare le loro offerte sotto forma di licenze concesse agli host francesi (OVHcloud, Orange, Scaleway, 3DS Outscale, ecc.).

L'adozione del Cloud dovrebbe permettere di accelerare l'attuazione degli impegni del governo in termini di trasformazione digitale delle amministrazioni.

I servizi digitali delle amministrazioni saranno ospitati su una delle due nuvole interne interministeriali dello Stato o sulle offerte di cloud proposte dai produttori che soddisfano rigorosi criteri di sicurezza. In particolare, ogni prodotto digitale che tratta dati sensibili, che si tratti dei dati personali dei cittadini francesi, dei dati economici relativi alle imprese francesi o delle applicazioni aziendali relative ai dipendenti pubblici dello Stato, deve essere ospitato sul cloud interno dello Stato o su un cloud industriale qualificato come **SecNumCloud** dall'ANSSI e protetto da qualsiasi regolamentazione extracomunitaria.

Sebbene le premesse siano delle migliori, allo stato attuale le cose stanno diversamente. Infatti, Google Cloud ha firmato un accordo con Thales nell'ottobre 2021. Microsoft, da parte sua, ha unito le forze con Orange e Capgemini attraverso un'entità dedicata, chiamata "*Bleu*", la cui data di lancio è ancora sconosciuta in questo momento. Solo Amazon non ha ancora annunciato una partnership nel panorama francese.



Perciò, nonostante la retorica del governo francese ruoti attorno al concetto di “cloud de confiance” (cloud di fiducia), resta da capire quanto realisticamente il cloud nazionale francese sia affrancato da ingerenze di terzi. Gli analisti e gli esperti sono scettici e sostengono che la struttura della strategia descritta non sia sufficiente e che non ci si possa neanche appellare ai cosiddetti “*trusted cloud principles*” (20) sanciti dai grandi CSP come AWS, Google, Microsoft, Cisco e molti altri. Di fatto, questi principi riguardano la parte di sicurezza operativa, ma non impediscono allo stato americano di richiedere al fornitore l'accesso ai dati ovunque essi si trovino. Questo implica che tecnologicamente il provider avrà sempre la possibilità di accedere ai dati.

Il terzo pilastro della strategia Cloud dello Stato consiste nel sostegno diretto a progetti ad alto valore aggiunto nel quadro del quarto programma di investimenti per il futuro e France Relance, il corrispettivo francese del PNRR italiano. Questa azione identifica e sostiene progetti industriali per lo sviluppo di tecnologie cloud in Francia. Si rivolge a tecnologie critiche come le soluzioni PaaS per la diffusione dell'intelligenza artificiale e dei big data o le suite di software per il lavoro collaborativo e dovrebbe permettere all'Europa e alla Francia di progredire nella sua sovranità tecnologica. In quest'ottica, a inizio novembre 2021 il segretario di stato francese per la transizione digitale, Cédric O, ha annunciato un piano d'investimenti da 1,8 miliardi di euro per sostenere la filiera del cloud francese.

20 Trusted Cloud Principles, 2021 <https://trustedcloudprinciples.com/principles/>



Il mercato del cloud: gli USA la fanno da padrone

Il mercato del cloud globale ha fortemente risentito in maniera positiva della pandemia da COVID-19, dato il fatto che la quasi totalità delle attività economiche hanno dovuto adattarsi a pratiche di lavoro principalmente in remoto. Questo ha quindi comportato una forte spinta verso la digitalizzazione dei processi produttivi ed in particolar modo dell'archiviazione dei dati. In Italia, come riportato dal Cloud Transformation Hub del Politecnico di Milano, il mercato dei servizi cloud in Italia è cresciuto del 16% nel solo 2021. Il centro studi prevede anche una spesa totale di circa 3.84 miliardi di euro, con circa 1.9 miliardi stanziati dal governo Italiano per promuovere la migrazione dei dati e dei servizi della pubblica amministrazione sul cloud nei prossimi 5 anni. Il trend del mercato nostrano era stato tra l'altro anticipato da forti investimenti messi in campo da multinazionali come Microsoft, che nello specifico ha investito a Maggio 2020 ben 1.5 miliardi di euro in servizi cloud in Italia. Non solo, la compagnia fondata da Bill Gates ha anche stilato un piano quinquennale che prevede di aumentare la propria offerta di servizi cloud, programmi di digital skills, smart-working e programmi di intelligenza artificiale per le piccole e medie imprese.

Dal punto di vista Europeo, invece, il mercato del cloud computing punta a sorpassare i 140 miliardi di dollari entro il 2028 in termini di volumi. In particolar modo è il segmento dell'Infrastructure as a Service (IaaS) a crescere di un consistente 15% dal 2021 al 2028, considerando l'importanza di questi servizi cloud per le imprese di livello aziendale. Interessante notare come entro il 2028, le piccole e medie imprese (SMEs) avranno una quota di mercato del 30%, considerando anche i consistenti finanziamenti pubblici che proprio le PMI riceveranno nel prossimo decennio in progetti di digitalizzazione.

In termini di provider globali, non sorprende il fatto che siano aziende USA e Cinesi a controllare la gran parte del mercato cloud in termini di quota di mercato. Nonostante sia molto più famoso come e-commerce, Amazon è stato in realtà anche uno dei pionieri del cloud commerciale.

La sua divisione Amazon Web Services (AWS) è infatti il leader mondiale nel settore, con un incasso di circa 16 miliardi di dollari nel solo Q3 2021, registrando una crescita del 39% rispetto all'anno passato. In un mercato da 150 miliardi di dollari annui, i servizi cloud di Mr Bezos ammontano infatti al 32% dell'intero settore cloud, seguiti da Microsoft Azure con il 20%. Google Cloud chiude il podio con un market share del 9%, mentre Alibaba Cloud, azienda cinese famosa anch'essa per il suo servizio di e-commerce, si piazza al quarto posto con un 6%. Chiudono la classifica IBM Cloud (5% - USA), Salesforce (3% - USA), Tencent Cloud (2% - China) ed Oracle (2% - USA).

Proprio all'interno di questo contesto tecnologico e geopolitico rientrano le iniziative europee volte a creare una sovranità specialmente nel campo del cloud e dell'intelligenza artificiale. Se da un punto di vista di mercato "reale" i player europei sono lontani dal competere con Cina e Stati Uniti, la Commissione Von der Leyen sta quindi tentando di rafforzare il settore tecnologico europeo sia tramite ingenti investimenti pubblici che tramite strumenti legislativi volti a regolamentare più strettamente il mercato europeo comune.



7. PROPOSTE DI POLICY

Al fine di sostanziare l'analisi appena svolta vengono riportate quelle che, a nostro avviso, sono le questioni più impellenti da affrontare per perfezionare *la migrazione dei dati della Pubblica Amministrazione al cloud*.

7.1. Inserire la Strategia Cloud Italia all'interno di un approccio olistico

Se è vero che la migrazione al cloud della PA possa portare numerosi benefici è anche vero che questa strategia vada inserita in un contesto più ampio. Occorre perciò tenere in conto aspetti ugualmente importanti che supportino la riforma dall'esterno. Basti pensare alle competenze digitali necessarie, alla necessità di una banda larga, se non ultralarga, per poter operare correttamente il cloud e ad un più generale ripensamento dei processi burocratici tipici dell'Amministrazione Pubblica.

Nonostante gli obiettivi sanciti da Italia Digitale 2026 (21) siano molto ambiziosi e si riscontri la volontà che almeno il 70% della popolazione sia digitalmente abile; il 75% delle PA italiane utilizza servizi cloud e tutte le famiglie italiane usufruiscono di reti a banda ultralarga, essi potrebbero essere facilmente irraggiungibili.

Per esempio, come ha reso noto l'**Unione Nazionale Comuni Comunità Enti Montani** (Uncem), il 75% dei comuni montani non possiede le infrastrutture adeguate per effettuare un celere passaggio al cloud a meno che non siano dotati di una rete a banda ultralarga gratuita (22).

La trasformazione digitale dell'Amministrazione Pubblica, braccio statale più vicino al cittadino, va letta con un'ottica di semplificazione e miglioramento del rapporto tra le Amministrazioni e i cittadini stessi.

21 Ministro per l'innovazione tecnologica e la transizione digitale, Obiettivi e iniziative per il digitale nel Piano nazionale di ripresa e resilienza, 2021 <https://innovazione.gov.it/dipartimento/focus/italia-digitale-2026/>

22 Unione Nazionale Comuni Comunità Enti Montani, Comuni con server sotto la scrivania degli uffici, uncem: cloud e sicurezza dati pubblici, in due terzi di italia, si fanno solo con buona infrastruttura, 4 agosto 2021 <https://uncem.it/comuni-con-server-sotto-la-scrivania-degli-uffici-uncem-cloud-e-sicurezza-dati-pubblici-in-due-terzi-di-italia-si-fanno-solo-con-buona-infrastruttura/>

Il cosiddetto *e-Government* non può essere raggiunto meramente adottando soluzioni ICT e applicandole a processi incompatibili con le stesse. I processi burocratici tradizionali sono pieni di attività non a valore aggiunto (ad esempio l'imposizione di requisiti documentali superflui rispetto al servizio richiesto, frequente rimando a altri enti amministrativi ecc.) che comportano una diminuzione di efficienza anche del personale addetto allo svolgimento di queste attività con un conseguente aumento dei costi e dei tempi per completare un servizio. Perciò, per migliorare l'efficienza, la trasparenza e la qualità dei servizi finali e soprattutto diminuire la complessità dei processi burocratici a vantaggio sia degli utenti esterni che di quelli interni, **è necessario un ripensamento generale dei procedimenti amministrativi.**

Proposta programmatica:

- Identificare le aree grigie e assicurare una copertura della rete a banda ultralarga su tutto il suolo nazionale. Ciò deve avvenire simultaneamente, se non prima, all'adozione di soluzioni cloud della PA.
- Semplificare le procedure autorizzative per la realizzazione delle reti, in particolare nei comuni montani.
- Adattare, alla luce di un riesame, i processi burocratici ai vantaggi che comportano le tecnologie ICT, nel nostro caso al cloud, scartando quei procedimenti non a valore aggiunto e quando possibile prevedere procedure standard.

7.2. Competenze digitali

Come ampiamente descritto, un uso ampio e pervasivo delle tecnologie digitali nei processi operativi della PA rappresenta senza dubbio un'importante opportunità di crescita economica. L'assenza di una cultura del digitale e dell'innovazione condivisa rende difficile coglierla appieno. È prioritario, in questo contesto, intervenire in modo incisivo sulle competenze digitali attraverso la definizione di interventi mirati e caratterizzati da tempistiche ben precise. In questo scenario si inserisce il progetto "Competenze digitali per la PA" avviato nel 2017 dal Dipartimento della funzione pubblica nell'ambito del PON Governance, che mira al consolidamento delle competenze digitali comuni a tutti i dipendenti pubblici (non professionisti ICT).

Ad oggi, questo progetto si basa su tre pilastri:

1. **Definizione e aggiornamento continuo del Syllabus** che descrive il set minimo di competenze digitali di base per ciascun dipendente pubblico.
2. **La realizzazione di una piattaforma applicativa** per l'erogazione via web di test di verifica e di valutazione dell'apprendimento.
3. Supporto all'erogazione della formazione attraverso la **creazione di un Catalogo** che raccoglie moduli formativi, volti a colmare le carenze di competenze digitali rilevate in fase di autoverifica.

Essendo ambizioso e complesso, riteniamo che questo progetto debba però essere associato ad un investimento più cospicuo e anticipato di risorse.

Proposta programmatica:

- Un sistema di autocontrollo, che permetta di fotografare il livello "baseline" delle competenze digitali possedute oggi dai dipendenti della PA.
- Valutare nel tempo come l'insieme degli interventi mirati sopra descritti vadano ad accrescere il livello minimo di competenze richieste e definire degli obiettivi chiari in merito alle stesse.
- Definire una curva di apprendimento necessaria al raggiungimento di determinate competenze, in modo tale da riuscire a formare sempre più figure in grado di rispondere ai nuovi bisogni di un settore in cambiamento.

7.3. Il nodo dell'inter-operabilità

In conclusione, è opportuno porre l'attenzione su una questione lasciata aperta, ma meritevole di approfondimento: interoperabilità e rapporti con CSP stranieri.

Interoperabilità dei servizi significa avere dei dati che sono in grado di parlare tutti la stessa lingua, in grado cioè di attribuire alle informazioni lo stesso significato. Questo presupposto è reso complicato nel momento in cui ci si appoggia a diversi i Cloud service provider (CSP) senza avere una e ben definita strategia organica.

Infatti, la necessità dell'interoperabilità nasce dall'esigenza di evitare una situazione di lock-in del venditori, tale per cui il cliente si trova nella condizione di non poter acquistare analoghi beni o servizi da un fornitore differente senza dover sostenere rilevanti costi e rischi per effettuare questo passaggio.

Come anticipato precedentemente, i CSP qualificati possono, oltre ai poli strategici nazionali e ai Cloud service provider del Lotto 1, fornire infrastruttura Cloud alla pubblica amministrazione. AGID ha delineato un percorso di qualificazione per i CSP della PA, affinché le pubbliche amministrazioni possano adottare infrastrutture Cloud di qualità e con caratteristiche omogenee.

Proposta programmatica:

- La standardizzazione e la definizioni di “formati aperti” che evitino situazioni di lock-in, con definizioni precise già integrate a livello progettuale (non solo in merito al trasferimento di dati statici, ma soprattutto di applicazioni con annesse componenti)

8. CONCLUSIONI

Il paper ha l'obiettivo di fornire un'analisi della Strategia Cloud Italia e di aspetti che la riguardano in modo diretto e indiretto. Per i primi, sono stati citati i rischi e le opportunità legati al piano del Ministro Colao e la strada normativa e strategica che ha portato all'elaborazione della Strategia stessa. Per i secondi, ci si è soffermati sulle criticità esogene, come i problemi legati ai CSP stranieri e in particolare a quelli americani e alla mancanza di competenze digitali adeguate. Come si è visto, alcune criticità sono intrinseche nella natura stessa del cloud computing mentre altre sono di matrice puramente strategica.

Perciò, l'adozione del Cloud computing nel settore pubblico richiede un'analisi approfondita e sistematica circa il modello di implementazione e servizio cloud appropriato (privato, pubblico, community, ibrido/IaaS, PaaS, SaaS), tenendo conto delle caratteristiche, vantaggi e svantaggi di ogni modello. Inoltre, richiede un'analisi adeguata dei requisiti e delle priorità dell'autorità pubblica in considerazione del carico di lavoro IT complessivo e delle applicazioni da migrare al cloud, poiché non tutte le applicazioni potrebbero essere in grado di funzionare correttamente nel cloud. Dovrebbero essere esaminate le questioni relative a sicurezza, privacy, integrità, disponibilità e conformità alle leggi e ai regolamenti esistenti. Infine, la selezione del fornitore di cloud (o dei fornitori) è di grande importanza. Tutto ciò sembra essere stato ben ponderato all'interno della Strategia Cloud Italia; resta quindi da vedere, una volta messa in pratica, come reagiranno le infrastrutture e l'apparato burocratico a un simile cambiamento.

Mentre le organizzazioni private sono più veloci nell'adozione e monetizzazione delle nuove tecnologie e nell'adozione del cloud, le organizzazioni pubbliche giocano su un terreno diverso dettato dalla generazione di valore per i cittadini e le imprese e da una legislazione molto più restrittiva. Inoltre, se da un lato è vero che l'adozione di tecnologie ICT, come il cloud, costituiscono il reale fattore abilitante per una concreta modernizzazione della pubblica amministrazione, dall'altro è anche vero che la spinta verso la semplificazione e la revisione dei processi amministrativi non può derivare meramente dall'adozione di modalità innovative di fruizione delle tecnologie ICT. Si può perciò affermare che il cloud non costituisce la soluzione ma lo strumento. Lo strumento adeguato per la digitalizzazione e la dematerializzazione ma che comporta una complessità organizzativa che la PA può gestire solo se presuppone un generale ripensamento dei processi amministrativi, adeguatamente adattati alle implicazioni del cloud.

BIBLIOGRAFIA

- AgID, CIRCOLARE N. 2 del 9 aprile 2018
https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/1811512344300__OCircolare+2-2018_Criteri+per+la+qualificazione+dei+Cloud+Service+Provider+per+la+PA.pdf
- AgID, CIRCOLARE N. 3 del 9 aprile 2018
https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/1811512372100__OCircolare+3-2018_Criteri+per+la+qualificazione+di+servizi+SaaS+per+il+Cloud+della+PA+%2802%29.pdf
- AgID, Connettività <https://www.agid.gov.it/it/infrastrutture/sistema-pubblico-connettivita/connettivita>
- AgID, Piano triennale per l'informatica nella Pubblica amministrazione 2017-2019
https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2017-2019/doc/01_piano-triennale-per-informatica-nella-pa.html
- AgID, Piano triennale per l'informatica nella Pubblica amministrazione 2019-2021
https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2019-2021/03_infrastrutture.html#cloud-della-pa
- AgID, Sistema Pubblico di Connettività
<https://www.agid.gov.it/it/infrastrutture/sistema-pubblico-connettivita>
- AWS, AWS GovCloud (US) <https://aws.amazon.com/it/govcloud-us/?whats-new-ess.sort-by=item.additionalFields.postDateTime&whats-new-ess.sort-order=desc>
- Cloud.Gov, Infrastructure under cloud.gov
<https://cloud.gov/docs/computingtechnology/iaas/>
- Compagnucci S., Massaro G., Osborn T., Principali L., Salerno D. (2021) Una strategia cloud per un'Italia più competitiva e sicura, Istituto per la competitività
- DECRETO-LEGGE 16 luglio 2020, n. 76
<https://www.gazzettaufficiale.it/eli/id/2020/07/16/20G00096/sg>
- Dipartimento per la Trasformazione Digitale, Strategia Cloud Italia Documento sintetico di indirizzo strategico per l'implementazione e il controllo del Cloud della PA <https://assets.innovazione.gov.it/1634299755-strategiacloudit.pdf>

- Dotto S., Mezzacapo G., Rencricca O., Consip: "Cloud e Spc, le gare che faranno la spina dorsale della nuova PA", 31 maggio 2016 https://www.forumpa.it/pa-digitale/consip-cloud-e-spc-le-gare-che-faranno-la-spina-dorsale-della-nuova-pa/?__hstc=254168151.18fdd7898f3eaf318a70388b699db9e5.1632210419509.1634976094748.1634982297975.3&__hssc=254168151.1.1634982297975&__hsfp=674959255&_ga=2.124641928.306647987.1634976094-1710119802.1632210419
- Gianni Dragoni, "Sogei polo strategico per la PA digitale" - Intervista a Andrea Quacivi, il Sole 24 ore, 28 marzo 2019 <https://www.sogei.it/it/sogei-homepage/azienda/sala-stampa/Articolieinterviste/articoli-e-interviste-2019/-sogei-polo-strategico-per-la-pa-digitale---intervista-a-andrea.html>
- Gouvernement français, Stratégie nationale pour le cloud, France Relance, 17 maggio 2021 <https://www.numerique.gouv.fr/uploads/Strategie-nationale-pour-le-cloud.pdf>
- Ministro per l'innovazione tecnologica e la transizione digitale, Obiettivi e iniziative per il digitale nel Piano nazionale di ripresa e resilienza, 2021 <https://innovazione.gov.it/dipartimento/focus/italia-digitale-2026/>
- MITRE, AWS GovCloud Resource and Cost Analysis, gennaio 2020 <https://apps.dtic.mil/sti/pdfs/AD1114483.pdf>
- Morati P., Cloud First, La PA che viaggia verso la nuvola, innovazione.PA, 25 giugno 2020
- Zaharia-Rădulescu A. M., Radu I. (2017) Cloud computing and public administration: approaches in several European countries, De Gruyter
- DOI: 10.1515/picbe-2017-0078
- Nanos I., Manthou V., Androutsou E. (2019) Cloud Computing Adoption Decision in E-government. In: Sifaleras A., Petridis K. (eds) Operational Research in the Digital Era – ICT Challenges. Springer Proceedings in Business and Economics. Springer, Cham. https://doi.org/10.1007/978-3-319-95666-4_9
- Piano Nazionale di Ripresa e Resilienza, 12 gennaio 2021 https://www.governo.it/sites/new.governo.it/files/PNRR_2021_0.pdf
- Piano Nazionale di Ripresa e Resilienza, 23 aprile 2021 <https://www.governo.it/sites/governo.it/files/PNRR.pdf>

- Presidenza del Consiglio dei Ministri, Strategia per la crescita digitale 2014-2020, 3 marzo 2015
https://www.agid.gov.it/sites/default/files/repository_files/documentazione/strat_crescita_digit_3marzo_0.pdf
- Trusted Cloud Principles, 2021
<https://trustedcloudprinciples.com/principles/>
- Unione Nazionale Comuni Comunità Enti Montani, Comuni con server sotto la scrivania degli uffici, uncem: cloud e sicurezza dati pubblici, in due terzi di italia, si fanno solo con buona infrastruttura, 4 agosto 2021 <https://uncem.it/comuni-con-server-sotto-la-scrivania-degli-uffici-uncem-cloud-e-sicurezza-dati-pubblici-in-due-terzi-di-italia-si-fanno-solo-con-buona-infrastruttura/>
- Vivek Kundra, Federal cloud computing strategy, 8 febbraio 2011
https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud--strategy.pdf

AWARE

www.awarethinktank.it

info@awarethinktank.it



Febbraio 2022