Videosorveglianza in cloud, un obbligo per le P.A.?

di Angelo Carpani (*)

1. INTRODUZIONE

Nella mia attività professionale, nella quale mi occupo quasi esclusivamente di progettazione di impianti di videosorveglianza in ambito comunale, mi sono imbattuto di recente per la prima volta in un Comune il quale, nel proprio "Piano triennale per l'informatica" (dopo vedremo di cosa si tratta), ha stabilito di non ricorrere più all'adozione di server "fisici" per la gestione e l'archiviazione dei dati ritenendo di ottenere notevoli risparmi in termini di hardware, energia consumata, manutenzione, ecc. senza la necessità di avere locali idonei ed annullando qualsiasi generazione di rumore e di calore.

Si tratta di un passaggio importante e che può contrassegnare l'inizio di una vera e propria ***rivoluzione*** nell'ambito delle Pubbliche Amministrazioni che sceglieranno i servizi Cloud, sia per infrastrutture che per quanto riguarda le soluzioni software e le piattaforme.

Senza la pretesa di trattare in modo esaustivo l'argomento, vediamo di cosa si tratta, sia da un punto di vista legislativo che tecnico, anche perché sul sito web dell'**AgID** (**A**genzia per l'Italia **D**igitale) si trovano molte informazioni al riguardo.

2. L'AGID ED IL PIANO TRIENNALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE 2019 -2021

L'Agenzia per l'Italia Digitale (AgiD) è un'agenzia tecnica che fa capo alla Presidenza del Consiglio, che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica. AgID ha il compito di coordinare le amministrazioni nel percorso di attuazione del **Piano Triennale per l'informatica della Pubblica Amministrazione**, favorendo la trasformazione digitale del Paese.

La **strategia Cloud della PA** nasce per favorire l'adozione del modello del *cloud computing* nelle pubbliche amministrazioni italiane, in linea con le indicazioni della Strategia per la Crescita digitale del Paese e con le previsioni del Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019 - 2021, e per qualificare servizi e infrastrutture cloud secondo specifici parametri di sicurezza e affidabilità idonei per le esigenze della PA.

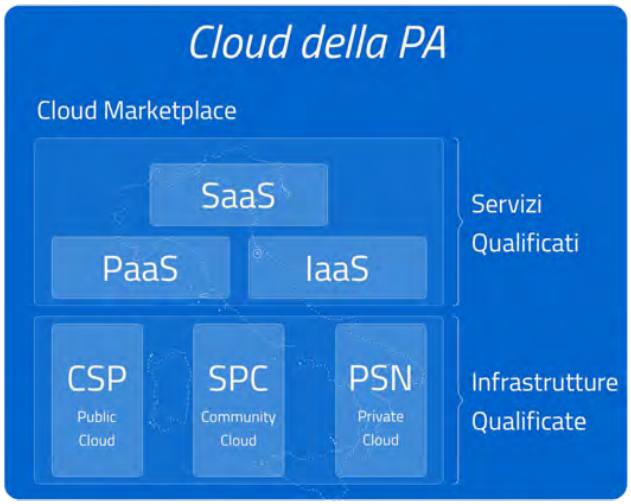
La strategia cloud delineata da AGID prevede un percorso di qualificazione per i soggetti pubblici e privati che intendono fornire infrastrutture e servizi Cloud alla Pubblica Amministrazione, affinchè queste ultime possano adottare servizi e infrastrutture di cloud computing omogenei, che rispettino elevati standard di sicurezza, efficienza ed affidabilità.

A decorrere dal 1° aprile 2019, le Amministrazioni Pubbliche (PA) possono acquisire esclusivamente servizi cloud qualificati da AgID e pubblicati nel **Cloud Marketplace** (il catalogo dei servizi cloud qualificati).

(*) Angelo Carpani, libero professionista, laureato in Ingegneria elettronica presso il Politecnico di Milano, iscritto all'Ordine degli Ingegneri della Provincia di Como (n. 2368 sez.A), esperto nella progettazione di impianti di videosorveglianza in ambito comunale.

3. IL MODELLO CLOUD DELLA PA

Al fine di incrementare l'adozione del cloud nella PA, il **Piano Triennale per l'informatica nella Pubblica Amministrazione 2017 - 2019** ha introdotto il **Modello Cloud della PA** che descrive l'insieme di infrastrutture IT e servizi cloud qualificati da AGID a disposizione della PA, secondo una strategia che prevede la realizzazione di tale modello, la definizione e attuazione del programma nazionale di abilitazione al Cloud della PA e l'applicazione del *principio* ***cloud first***.



Come illustrato nella figura, il Modello Cloud della PA è composto da:

- **Servizi Qualificati** da AgID consultabili mediante il *Cloud Marketplace* suddivisi in ***IaaS*** *(**I**nfrastructure **a**s **a** **S**ervice),* ***PaaS*** *(**P**latform **a**s **a** **S**ervice) e* ***SaaS*** *(**S**oftware **a**s **a** **S**ervice).*
- **Infrastrutture Qualificate** da AgID quali i ***C****loud* ***S****ervice* ***P****rovider (CSP)*, i ***P****oli* ***S****trategici* ***N****azionali (PSN)* e l'infrastruttura di *Community Cloud*.

3.1 I Servizi Qualificati

IaaS, SaaS e PaaS possono essere considerati gli elementi centrali dell'informatica moderna, non più legata esclusivamente a macchine fisiche e a logiche "on premise", ovvero di server e apparecchiature possedute e controllate privatamente, ma che sempre più trova il suo sviluppo nel *cloud computing* tradizionale, fatto di **infrastrutture** IT controllate da provider di servizi esterni che mettono a disposizione risorse di elaborazione in funzione delle necessità.

Qual è quindi la differenza tra servizi cloud IaaS, PaaS e SaaS?

SaaS (Software as a Service)

Per *Software as a Service* si intendono quelle applicazioni **Software** accessibili tramite Internet sfruttando diverse tipologie di dispositivi (Desktop, Mobile, etc). La facoltà fornita al consumatore è quindi quella di utilizzare le applicazioni del fornitore funzionanti su un'infrastruttura cloud. Le applicazioni sono accessibili da diversi dispositivi attraverso un'interfaccia leggera come, ad esempio, un'applicazione email su browser, oppure da programmi dotati di apposita interfaccia. L'obiettivo del **cloud Saas** è quindi quello di fornire agli utenti, siano essi *consumer o business*, un'applicazione accessibile ovunque sia disponibile una connessione a Internet. Il software e i dati risiedono su cluster di server che erogano il servizio senza la necessità di memorizzare i dati in locale sulla macchina.

IaaS (Infrastructure as a Service)

Per I*nfrastructure as a Service* si intendono quelle **Infrastrutture** tecnologiche fisiche e virtuali in grado di fornire risorse di computing, networking e storage da remoto e mediante API (Application Programming Interface). La facoltà fornita al consumatore è quindi quella di acquisire elaborazione, memoria, rete e altre risorse fondamentali di calcolo, inclusi sistemi operativi e applicazioni. Chi si affida a un servizio **cloud IaaS** non ha quindi più alcuna necessità di possedere le macchine e manutenerle: è il provider di servizi, infatti, a mettere a disposizione delle risorse computazionali sotto forma di **macchine virtuali** affittate in base alle singole esigenze e sulle quali possono essere installati sistemi operativi e software esattamente come su un'infrastruttura proprietaria, con l'enorme vantaggio di non doversi più preoccupare di alcun aspetto legato al possesso fisico di un parco macchine.

PaaS (Platform as a Service)

Per *Platform as a Service* si intendono le **Piattaforme** per sviluppare, testare e distribuire le applicazioni su internet. La facoltà fornita al consumatore è quindi quella di distribuire sull'infrastruttura *cloud* applicazioni create in proprio oppure acquisite da terzi, utilizzando linguaggi di programmazione, librerie, servizi e strumenti supportati dal fornitore. Il **cloud PaaS** offre quindi tutti gli strumenti necessari per la creazione, lo sviluppo e la distribuzione delle applicazioni senza la necessità di disporre di un'infrastruttura fisica né di dover installare sistemi operativi o ambienti di sviluppo, lasciando così piena libertà di sviluppo all'interno delle caratteristiche offerte dalla piattaforma.

3.2 Le Infrastrutture Qualificate

Il fornitore di servizi cloud – Cloud Service Provider (CSP)

I Cloud service provider (CSP) sono i fornitori di servizi cloud qualificati da AGID, che possono erogare servizi di tipo **Public Cloud** alle amministrazioni. Le qualificazioni AGID assicurano che le infrastrutture e i servizi dei CSP siano sviluppati ed operanti secondo criteri minimi di affidabilità e sicurezza considerati necessari per i servizi digitali della PA.

Il Sistema Pubblico di Connettività (SPC)

E' un insieme di infrastrutture tecnologiche e di regole tecniche che ha lo scopo di "federare" le infrastrutture ICT delle Pubbliche amministrazioni al fine di realizzare servizi integrati mediante regole e servizi condivisi. Tale integrazione permette di risparmiare sui costi e sui tempi e di realizzare i servizi finali centrati sull'utente, evitando richieste continue di dati da parte delle amministrazioni, oltre che duplicazioni di informazioni e controlli.

I Poli Strategici Nazionali (PSN)

Per **PSN** si intende il soggetto titolare dell'insieme di infrastrutture IT (centralizzate o distribuite), ad alta disponibilità, di proprietà pubblica, eletto a Polo Strategico Nazionale dalla Presidenza del Consiglio dei Ministri e qualificato da AgID ad erogare, in maniera continuativa e sistematica, ad altre amministrazioni:

- servizi infrastrutturali on-demand (es. housing, hosting, IaaS, PaaS, SaaS, ecc.);
- servizi di disaster recovery e business continuity;
- servizi di gestione della sicurezza IT;
- servizi di assistenza ai fruitori dei servizi erogati.

Presso i PSN dovranno essere presenti e gestite le principali infrastrutture ICT (hardware, software, connettività) messe a disposizione delle altre amministrazioni, senza vincoli rispetto alla localizzazione sul territorio nazionale.

4. La videosorveglianza e il principio del "cloud first"

Veniamo allora alla fatidica domanda: l**a videosorveglianza in cloud è un obbligo per le PA?**

Il nuovo Piano triennale per l'informatica nella pubblica amministrazione (2019-2021) prevede l'applicazione del **principio "cloud first"**: "Le pubbliche amministrazioni, in fase di definizione di un nuovo progetto, e/o di sviluppo di nuovi servizi, in via prioritaria devono valutare l'adozione del paradigma cloud prima di qualsiasi altra tecnologia, tenendo conto della necessità di prevenire il rischio di *lock-in*[1]. Dovranno altresì valutare il ricorso al cloud di tipo pubblico, privato o ibrido in relazione alla natura dei dati trattati e ai relativi requisiti di confidenzialità".

1 Rischio di dipendenza esclusiva dal fornitore

WISENET WAVE

SELEZIONA. SPOSTA. RILASCIA. VISUALIZZA.

TUTTO QUI.

Una piattaforma VMS che già conosci.
Prima di utilizzarla.

Tutto è Drag & Drop.
Sfoglia le immagini per controllare tutte le telecamere live.
Clicca sulla Time Line per accedere immediatamente alle immagini registrate.
Trova immediatamente le immagini che ti interessano con la funzione Smart Search.
WISENET WAVE è leggero, si installa in pochi minuti e ottimizza l'utilizzo delle risorse hardware.
Una User Interface semplice ed intuitiva che guida l'utente attraverso le funzionalità complete.

We move with trust.

Scopri subito Wisenet WAVE, scrivi a hte.italy@hanwha.com.

Hanwha Techwin

Sulla base tale principio, questo non significa che l'impiego di server o NVR in loco, nelle applicazioni di videosorveglianza, siano vietati, ma che l'impiego del cloud deve essere prioritariamente valutato. Solo qualora il *"cloud first"* non soddisfi i criteri enunciati, si possono sempre utilizzare i sistemi tradizionali, anche con nuovi acquisti che, però, debbono essere adeguatamente giustificati (la mancata giustificazione può essere elemento di responsabilità contabile).
Il termine del 1° aprile, infatti, si riferisce solo agli acquisti dei servizi cloud, che debbono essere obbligatoriamente qualificati da AgID, e non ai casi, residui, nei quali si sia proceduto alla valutazione del *cloud first*" con esito negativo.

4. Criticità del cloud computing per la videosorveglianza

Il cloud, nell'ambito della trasformazione digitale, rappresenta una delle tecnologie cosiddette *disruptive*[2], che comporta notevoli vantaggi in termini di incremento di affidabilità dei sistemi, qualità dei servizi erogati, risparmi di spesa realizzabili attraverso l'opportunità della migrazione dei servizi esistenti verso il cloud e la possibilità di pagare soltanto gli effettivi consumi in cui, all'atto pratico, il Cliente paga solo ciò che usa *(pay-per-use)* e gli unici costi da sostenere dipendono dallo spazio utilizzato *(storage)* e dal traffico in uscita *(connettività richiesta)*. Le tecnologie Cloud, oltre alla flessibilità, dispongono di una potenza di calcolo e risorse irraggiungibili dalle solite infrastrutture *on-premise*, mettendo in sicurezza le informazioni più importanti, secondo uno schema di salvataggio e ripristino tipico delle infrastrutture di *Disaster Recovery*[3].

Tuttavia, nella realizzazione di impianti di videosorveglianza in cloud, soprattutto in ambito cittadino, per via della presenza di numerose telecamere impiegate, per di più a risoluzione sempre più elevata (ad es. Ultra HD – 4K), vanno tenute in conto alcune criticità.

La **prima criticità** è legata al *networking* e all'internet service provider (ISP) utilizzato per l'accesso al cloud provider; il numero delle telecamere che possono essere collegate dipende dal tipo di connessione (es. fibra, adsl, ecc.) e anche sfruttando l'algoritmo di compressione H.265 (ad es. per le telecamere 4K) il numero delle stesse che possono essere collegate è sicuramente non elevato e dipende comunque dalle prestazioni e dalla qualità della connessione.

La **seconda criticità** riguarda lo *storage*. Anche se attualmente le memorie hanno un trend di costo per Terabyte continuamente in calo, lo storage richiesto è molto elevato in quanto, in base alla ***Direttiva del Ministero dell'Interno n.558/SICP ART/421.2/70 del 2 marzo 2012***, avente per oggetto i *Sistemi di videosorveglianza in ambito comunale*, i sistemi di videosorveglianza dovranno rispettare in ogni caso i requisiti di seguito riportati:

- capacità di banda necessaria al trasferimento delle immagini in funzione delle caratteristiche delle telecamere e della tecnologia della rete di trasporto;
- la memorizzazione delle immagini provenienti da tutte le telecamere al massimo frame rate possibile;

2 Il concetto di "disruptive technology" è stato introdotto per la prima volta da un articolo di Christensen ed altri, pubblicato su Harvard Business Review, nel 1995. Secondo gli autori "disruption" descrive un processo per cui un'impresa più piccola e con meno risorse è in grado di sfidare con successo le imprese dominanti un certo settore. Le imprese dominanti nel concentrarsi su come migliorare i propri prodotti e servizi per i clienti più esigenti (e di solito più redditizi), eccedono le esigenze di alcuni segmenti e ignorano i bisogni degli altri. I nuovi entranti, con intenti "disruptive", iniziano a soddisfare con successo quei segmenti trascurati e si ritagliano una posizione fornendo le funzionalità richieste dai segmenti ignorati dai dominanti, spesso a un prezzo inferiore. Le imprese dominanti, a caccia di una maggiore redditività nei segmenti più esigenti, non rispondono in maniera adeguata a questo attacco. I nuovi entranti quindi evolvono per soddisfare segmenti più elevati del mercato, offrendo le prestazioni che i clienti principali delle imprese dominanti richiedono, pur mantenendo i vantaggi che hanno determinato il loro primo successo. Quando i clienti tradizionali iniziano ad abbandonare le imprese dominanti per adottare in volumi le soluzioni offerte dai nuovi entranti, avviene la "disruption".

3 Con "disaster recovery" (in italiano: Recupero dal Disastro), in informatica ed in particolare nell'ambito della sicurezza informatica, si intende l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività.

- la registrazione delle immagini deve avvenire in forma cifrata, in accordo a quanto richiesto al paragrafo 3.3.1 comma t del "Provvedimento in materia di videosorveglianza" dell'8 Aprile 2010 del Garante per la Privacy (utilizzo di reti pubbliche e connessioni wireless), per garantirne la riservatezza e l'integrità;
- la capacità di storage deve essere dimensionata per la registrazione contemporanea di tutte le telecamere al massimo frame rate consentito dalle stesse e/o dalla connettività per un periodo di almeno 7 gg 24h.

La **terza criticità** riguarda l'aspetto regolatorio e le norme che i sistemi di videosorveglianza sono tenuti ad osservare, in particolare quelli legati alla *sicurezza* dei dati e alla *privacy* (GDPR). Usufruire di un servizio di cloud storage per la memorizzazione dei dati, in particolare per quelli personali o sensibili, può esporre il cliente a potenziali problemi di violazione della privacy: infatti i dati personali del cliente o delle immagini registrate dal sistema cliente vengono di fatto affidate ad un soggetto terzo con tutte le implicazioni del caso. In ottica **privacy e GDPR**, il provider deve rispondere in modo trasparente e prevedere che tutti i dati memorizzati rimangano di proprietà esclusiva del cliente. Stante questa logica, eventuali attività di accesso, condivisione, modifica e trasferimento devono essere ad esclusivo appannaggio del cliente stesso.