Pubblica Amministrazione che si trasforma: Cloud Computing, Federalismo, Interoperabilità

Roma, ForumPA 11 maggio 2011

*Alessandro Osnaghi, ASTRID - Comitato scientifico THINK***!**

Ringrazio gli organizzatori per avermi invitato a intervenire a questo convegno e mi chiedo quale contributo possa realmente dare su questi temi una persona che da molto tempo è solo un osservatore esterno, anche un po' distante, dei temi dell'informatizzazione della pubblica amministrazione. Cercherò di proporvi alcune riflessioni personali che sono state stimolate proprio da questo invito.

Cloud computing è termine molto ampio e una buzzword dai molteplici significati e tuttavia si basa su realtà tecnologiche ormai mature e potenzialmente dirompenti. Molti governi, tra cui quelli USA, UK e altri, hanno riconosciuto i potenziali benefici di questa discontinuità e hanno recentemente prodotto documenti di strategia per l'utilizzo del cloud computing da parte delle loro amministrazioni.

L'aspetto rilevante è che queste tecnologie consentono di erogare a domanda e in modo scalabile servizi infrastrutturali e applicativi attraverso la rete. Il Cloud computing si basa sulle tecnologie di virtualizzazione capaci di organizzare dinamicamente insiemi di risorse virtuali a beneficio delle applicazioni e dei servizi. Naturalmente questa tecnologia cambia anche il modo di sviluppare e distribuire le applicazioni.

Piuttosto che di *cloud computing* sarebbe appropriato parlare *di cloud services* perché nel cloud non è offerto il solo calcolo, ma molti altri servizi che secondo il NIST (National Institute of Standards and Technology) del governo degli Stati Uniti, sono classificati di tipo SaaS, PaaS o IaaS[1], servizi

[1] ***Cloud Software as a Service (SaaS)****. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.*

Cloud Platform as a Service (PaaS)*.The capability provided to the consumer is the ability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and* ***tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure*** *including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.*

Cloud Infrastructure as a Service (IaaS)*. The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).*

che sono erogati in internet dai Cloud Provider con modalità estremamente interessanti e innovative perché consentono di acquisire risorse scalabili e a domanda e di pagarle a tariffa in base all'effettivo utilizzo, trasformando costi di investimento e di gestione in soli costi di gestione.

Per raggiungere i servizi offerti dalla nuvola, quando ad esempio si virtualizza un server del sistema informativo o si acquisisce capacità di *storage*, le singole stazioni di lavoro dovranno accedere al server virtuale attraverso una rete a larga banda (quanto larga dipenderà dai singoli casi). La banda disponibile presso l'utenza è quindi un prerequisito del cloud computing. Non ha senso parlare di cloud computing, a livello infrastrutturale o di piattaforma o applicativo, se le stazioni di lavoro che restano nelle sedi dell'amministrazione non dispongono direttamente di una banda adeguata verso l'esterno.

La diffusione capillare nel Paese della banda larga è tema di discussione in altre sedi, ma per beneficiare delle tecnologie del cloud computing diventa essenziale che siano raggiunte dalla banda larga tutte le amministrazioni prima ancora dei singoli cittadini.

Le amministrazioni, come del resto le aziende, dal punto di vista delle dimensioni e delle possibilità/capacità di progettare e gestire sistemi informativi complessi, non sono tutte uguali; se però le consideriamo dal punto di vista degli adempimenti previsti dal Codice dell'amministrazione digitale (CAD), o dalla normativa sulla tutela dei dati personali, hanno tutte senza distinzioni gli stessi obblighi giuridici.

Proprio il CAD chiarisce quali sono le amministrazioni che lo devono applicare e che si devono fare direttamente carico di adempimenti complessi e costosi, infatti, all'Art. 2 *Finalità e ambito di applicazione*, il comma 2 rimanda all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, che recita:

"Per amministrazioni pubbliche si intendono tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale"

E questa elencazione è ribadita nel CAD stesso all'Art.1 *Definizioni* al comma 1 z).

Nel nostro paese le norme sull'uso delle tecnologie ICT da parte delle amministrazioni sono in alcuni casi formulate in modo ambiguo o impreciso e

spesso sono inapplicabili e disattese da parte dei soggetti interessati perché la loro attuazione implica costi di progettazione e di esercizio non proporzionati alle dimensioni dell'organizzazione e soprattutto richiede competenze tecniche e organizzative difficilmente accessibili a molte amministrazioni.

Mi piace sempre ricordare che, su un totale di circa 8100, circa 7500 Comuni hanno meno di 20.000 abitanti e quasi 6000 Comuni hanno meno di 5.000 abitanti. Le ASL sono circa 400 (il numero varia in continuazione) e le scuole sono circa 14.000.

Il costo di adeguamento alle norme non è proporzionato ai parametri dimensionali e molte amministrazioni sono nella pratica impossibilità di rispettare molti adempimenti anche nei casi in cui le norme rispondono a finalità d'interesse generale per la sicurezza del Paese. Ricordare che il CAD si applica a tutti, ai comuni, anche quelli piccoli e piccolissimi, e alle scuole di ogni ordine e grado, consente di pensare al **cloud computing come allo strumento per permettere a tutti di adeguarsi più facilmente e con costi minori a norme e regole tecniche che altrimenti sarebbero disattese**.

Per illustrare quest'affermazione utilizzo un esempio tratto dalle recenti modifiche apportate al CAD con l'introduzione dell'Art 50-bis *Continuità operativa* e le integrazioni dell'Art. 51 *Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni.*

L'Art. 50-bis è sicuramente un articolo fondamentale per la sicurezza generale dei sistemi da cui dipende il funzionamento del Paese e richiede alle amministrazioni, al comma 3 a) di redigere un piano di continuità operativa, *pur tenendo conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche*, e al comma 3 b) di predisporre un piano di disaster recovery, e affida a DigitPA il compito di verificare annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate. Inoltre richiede, al comma 4, che le amministrazioni adottino i piani dopo aver redatto appositi studi di fattibilità su cui è obbligatorio acquisire il parere di DigitPA.

Al di fuori della normativa sulla tutela dei dati personali una simile prescrizione generale effettivamente mancava ed è sicuramente nell'interesse del Paese che non siano persi dati essenziali al funzionamento della macchina amministrativa. Ma come pensare che ogni piccolo comune o ogni scuola possano singolarmente assicurare la continuità operativa e il disaster recovery, senza avere a disposizione adeguate competenze tecniche ed organizzative per dare esecuzione a obblighi di legge di questa complessità e per predisporre gli studi di fattibilità. A meno di non voler

considerare l'inciso "*pur tenendo conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche*" come una scappatoia per consentire di eludere l'obbligo.

Predisporre un modello di studio di fattibilità standard aiuterebbe, ad esempio, non solo queste amministrazioni a realizzare soluzioni conformi, ma anche DigitPA a ridurre la mole di lavoro necessaria per dare parere obbligatorio sugli studi di fattibilità e per verificare annualmente i piani di disaster recovery.

Piuttosto che imporre a tutti obblighi inattuabili, lo Stato **dovrebbe offrire soluzioni** e creare le condizioni perché siano resi disponibili alle amministrazioni servizi standard certificati e questo si potrebbe fare proprio utilizzando la tecnologia e i servizi offerti dal cloud computing.

Ad esempio - sempre che sia disponibile la banda larga - i server con le applicazioni e i dati delle scuole o dei piccoli-medi Comuni potrebbero essere virtualizzati e spostati nella nuvola trasferendo al gestore del servizio l'incombenza di assicurare la continuità operativa o il disaster recovery, cioè le funzioni di *disponibilità* del servizio. Recenti incidenti dovrebbero suggerire prudenza nell'adottare soluzioni non certificate, ma si tratta pur sempre di valutare quale sia il caso di rischio maggiore.

È necessario a questo punto, sempre utilizzando le definizioni[2] del NIST, considerare i diversi modelli di cloud computing.

Possiamo considerare il **cloud privato** come una delle tante evoluzioni tecnologiche che le organizzazioni dotate di grandi data center sono chiamate a fronteggiare periodicamente. In questi casi la responsabilità delle scelte di adozione di queste tecnologie è affidata ai Chief Information Officer (CIO) delle singole organizzazioni, si tratti di soggetti privati o di soggetti pubblici. In Italia diversamente dai paesi citati questo ruolo non esiste a livello di Governo centrale.

---

[2] ***Private cloud***. *The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.*

Community cloud. *The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations).It may be managed by the organizations or a third party and may exist on premise or off premise.*

Public cloud. *The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.*

Hybrid cloud. *The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).*

Nel caso della Pubblica amministrazione possiamo pensare a INPS o al Ministero delle Finanze o dell'Interno. I servizi cloud privati in questo caso sarebbero erogati sotto la responsabilità diretta dell'organizzazione stessa, in particolare dal punto di vista della sicurezza, e l'utilizzazione dei servizi avverrà da parte di utenze interne attraverso una rete privata. Il cloud privato offre la possibilità di consolidare infrastrutture, piattaforme e applicazioni per ottenere un beneficio di efficienza ed efficacia, tuttavia l'uso di queste nuove soluzioni tecnologiche e architetturali è relativamente trasparente ai servizi erogati agli utenti interni e esterni.

Non tutte le amministrazioni, come ho ricordato, sono dotate di veri e propri data center e di risorse e competenze informatiche adeguate alla complessità delle tecnologie da utilizzare, dei servizi da erogare e dei requisiti normativi da rispettare.

Per molti servizi, come ad esempio quelli di *storage* o di posta elettronica, il modello oggi proposto è quello del **cloud pubblico** e in questo caso, come già segnalato dal Garante, si presentano molte criticità, in particolare dal punto di vista dei requisiti di sicurezza richiesti, di conformità alle normative vigenti sul trattamento dei dati personali e dei dati sensibili e sulla disponibilità dei servizi.

Tornando alla realtà delle nostre amministrazioni, alle scuole, ai Comuni, alle Province, alle ASL, alle Regioni, ecc., in termini di utenza servita, alcune sono piccole, altre grandi, ma sono tutte incaricate degli stessi servizi e degli stessi compiti istituzionali e di gestione. Se quindi le consideriamo dal punto di vista funzionale si potrebbe affermare che gli enti omogenei dovrebbero, e potrebbero, avere sistemi informativi funzionalmente equivalenti, se non identici, che differiscono solo dal punto di vista dimensionale e dal punto di vista gestionale e spesso solo a causa di procedimenti amministrativi non standardizzati, ma che potrebbero esserlo.

In presenza del processo di federalismo istituzionale ed amministrativo in atto, se l'insieme dei sistemi informativi delle amministrazioni, che pure sono tenute al rispetto delle medesime norme, continuerà a non essere governato in termini di **standard dei dati**, di **progettualità sistemica** e di **pianificazione nazionale**, la tendenza alla differenziazione e alla frammentazione, con conseguente mancanza di interoperabilità, sarà ulteriormente accentuata e aggravata rispetto alla già molto critica situazione attuale.

In questa situazione il **cloud di comunità** è il modello di cloud computing che più corrisponde alle esigenze della Pubblica amministrazione intesa come insieme di organizzazioni distinte che operano in uno stesso contesto giuridico/amministrativo, che hanno analoghi requisiti di sicurezza, di

conformità e di policy e che potranno così interoperare tra loro attraverso infrastrutture, standard e servizi condivisi**.**

Non si tratta tanto di pensare a una nuvola "esclusiva dell'amministrazione" ma a un'infrastruttura tecnologica nazionale che renda disponibili **servizi certificati,** erogati da soggetti accreditati, che rispondono dal punto di vista funzionale, tecnico, contrattuale e soprattutto di fiducia, ai requisiti funzionali e normativi prescritti per le amministrazioni. Se, ad esempio, alcuni dati devono risiedere sul territorio nazionale, quest'opzione deve poter essere garantita.

Realizzare un cloud di comunità nell'ambito del quale i servizi sono erogati essenzialmente da soggetti privati accreditati non è solo complesso per gli aspetti tecnici organizzativi e di governance, ma soprattutto per la necessità di rivedere gli strumenti normativi e regolamentari abilitanti o di predisporne di nuovi. Ricordo che alcuni servizi critici, ad esempio quelli relativi alla firma digitale, sono stati affidati a soggetti privati fiduciari che operano in modo conforme al CAD e altri se ne potrebbero aggiungere, come ad esempio i servizi di Identity Management, anch'essi un prerequisito per il cloud computing e l'interoperabilità.

Per evidenziare alcune delle situazioni di criticità riprendo l'esempio di una scuola o di un piccolo comune che decidano di virtualizzare i loro server trasferendo quindi nella nuvola le basi dati che contengono dati personali (ad esempio l'anagrafe degli studenti o l'anagrafe demografica). Questo, alla condizione di sapere dove si trovano i dati, sarebbe possibile già ora e in questo modo queste amministrazioni potrebbero assicurarsi anche i servizi di continuità operativa e di disaster recovery.

Se tutto è trasferito nella nuvola presso un CSP (Cloud Service Provider), nella scuola o nel comune restano solo il router e le stazioni di lavoro e si accede al server virtuale attraverso i servizi di un ISP (Internet Service Provider).

Nei fatti il titolare del trattamento dati (il sindaco o il preside) può essere direttamente responsabile solo della loro certificazione, l'ISP ha nei fatti la responsabilità di garantire l'integrità e la confidenzialità nel trasferimento delle informazioni al CSP, mentre la responsabilità del controllo dell'accesso e della disponibilità, ma anche dell'integrità e confidenzialità è di fatto sotto il controllo diretto del CSP.

Questa situazione di fatto non corrisponde alla situazione di diritto perché in base alla normativa sulla tutela dei dati personali, il preside o il sindaco, titolari dei dati, restano oggi responsabili degli adempimenti relativi a tutti gli aspetti della sicurezza: l'autenticità del dato (certificazione), il controllo

dell'accesso, la confidenzialità, l'integrità e la disponibilità, che comporta appunto la continuità operativa ed il disaster recovery.

Esiste quindi una molteplicità di soggetti coinvolti ed è necessario chiedersi se e come possa essere gestita e/o semplificata la catena delle responsabilità giuridiche **almeno nell'ambito di una nuvola di comunità**. Non sono un giurista e queste riflessioni, sicuramente approssimative, vogliono solo evidenziare la necessità di affrontare con norme adeguate questa sfida tecnologica.

I processi di revisione/innovazione normativa sia a livello nazionale che a livello europeo sono inevitabilmente molto lunghi, tuttavia già in altri casi, ad esempio nel caso della firma digitale, abbiamo anticipato la normativa europea e forse anche in questo caso si potrebbe cercare di non frenare l'utilizzo di una tecnologia che potrebbe portare grandi benefici all'amministrazione italiana. Queste tecnologie sono qui per restare!

È oggi urgente riprendere un percorso già iniziato nella metà degli anni 90 con il progetto RUPA e proseguito con SPC e con la realizzazione dei servizi di supporto alla cooperazione applicativa SPCoop e lanciare uno **Studio di Fattibilità** che definisca l'architettura e l'infrastruttura tecnologica di un **cloud di comunità** per mettere gradualmente a disposizione delle amministrazioni adeguati servizi cloud IaaS, PaaS o SaaS.

La caratterizzazione di questi servizi non sarà esclusivamente di natura funzionale, molti servizi equivalenti saranno sicuramente disponibili anche nella nuvola pubblica, ma si dovrà trattare di servizi "garantiti" da un accreditamento dello Stato per quanto riguarda gli aspetti di conformità a requisiti normativi o di sicurezza o di qualità del servizio o di responsabilità legale, e basati su contratti standard in modo che il loro utilizzo garantisca automaticamente alle amministrazioni l'assolvimento degli obblighi di legge o di esigenze politico-strategiche del Paese.

Come avvenuto nei casi RUPA e SPC, allo Studio di Fattibilità dovrà seguire una legge istitutiva di un **Progetto nazionale e sistemico** finalizzato a realizzare l'infrastruttura tecnologica del Paese. Il progetto è tanto più necessario proprio in un'ottica di evoluzione federale dello Stato e, analogamente a quanto avviene in altri paesi, dovrebbe rispondere a un CIO (Chief Information Officer) che abbia adeguati poteri e strutture permanenti di governance e di gestione.

Personalmente ritengo che, coerentemente con il paradigma del cloud computing, l'investimento per realizzare i servizi cloud non competa alla parte pubblica, ma principalmente alle parti private accreditate. Tuttavia le amministrazioni dovranno far evolvere i loro sistemi informativi secondo un

piano preordinato dal Progetto nazionale in modo che sia garantito ai service provider il ritorno dell'investimento in tempi ragionevoli e certi.

È necessario trarre lezione dal recente passato in cui servizi infrastrutturali per il supporto alla cooperazione applicativa tra amministrazioni sono stati messi a disposizione, ma è mancato un piano organico e di incentivi per far evolvere nel senso della cooperazione i sistemi informativi delle amministrazioni. Ancor oggi, e vorrei sbagliarmi, tranne forse nell'ambito di alcune reti regionali, non sono in esercizio casi reali di cooperazione applicativa.

L'esperienza e la storia ci dicono che progetti di questa natura richiedono in Italia tempi epocali. L'idea della cooperazione applicativa è del 1996 e gli standard necessari sono consolidati da circa dieci anni. Posso solo augurare che l'evoluzione verso un cloud di comunità dell'amministrazione italiana non richieda altrettanto tempo: non ce lo possiamo permettere.

ALLEGATO

Art. 50-bis. Continuità operativa.

1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.

2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.

3. A tali fini, le pubbliche amministrazioni definiscono:
a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;
b) il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.

4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.

Art.51. *(**Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni**)*.

1. Con le regole tecniche adottate ai sensi dell'articolo 71 sono individuate le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture.
1-bis. DigitPA, ai fini dell'attuazione del comma 1:
a) raccorda le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;
b) promuove intese con le analoghe strutture internazionali;
c) segnala al Ministro per la pubblica amministrazione e l'innovazione il mancato rispetto delle regole tecniche di cui al comma 1 da parte delle pubbliche amministrazioni.";
d) dopo il comma 2, è aggiunto il seguente: "2-bis. Le amministrazioni hanno l'obbligo di aggiornare tempestivamente i dati nei propri archivi, non appena vengano a conoscenza dell'inesattezza degli stessi.".

2. I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.

omissis

6. Le disposizioni del presente codice non si applicano limitatamente all'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, e consultazioni elettorali. ***Con decreti del Presidente del Consiglio dei ministri, tenuto conto delle esigenze derivanti dalla natura delle proprie particolari funzioni, sono stabiliti le modalità, i limiti ed i tempi di applicazione delle disposizioni del presente Codice alla Presidenza del Consiglio dei Ministri, nonché all'Amministrazione economico-finanziaria.***