Comunicazione istituzionale e servizi digitali 3/2012

di Elisabetta Zuanelli

Il cloud computing: definizioni, modelli, vantaggi e rischi

1. Definizioni 2. I vantaggi della nuvola 3. Le tipologie di "cloud" 4.Il dibattito 5. La sicurezza e la privacy 6. I modelli di *cloud computing* e i criteri da verificare

Il *cloud computing*,"elaborazione a nuvola", è un'immaginifica bolla concettuale nella quale l'unica certezza definitoria è data dal riferimento a servizi infrastrutturali, elaborativi, trasmissivi, relazionali, gestiti attraverso piattaforme Internet: servizi digitali, *on demand*, su richiesta e *pay per use*, pagamento per uso. In generale, è una metafora per indicare Internet.

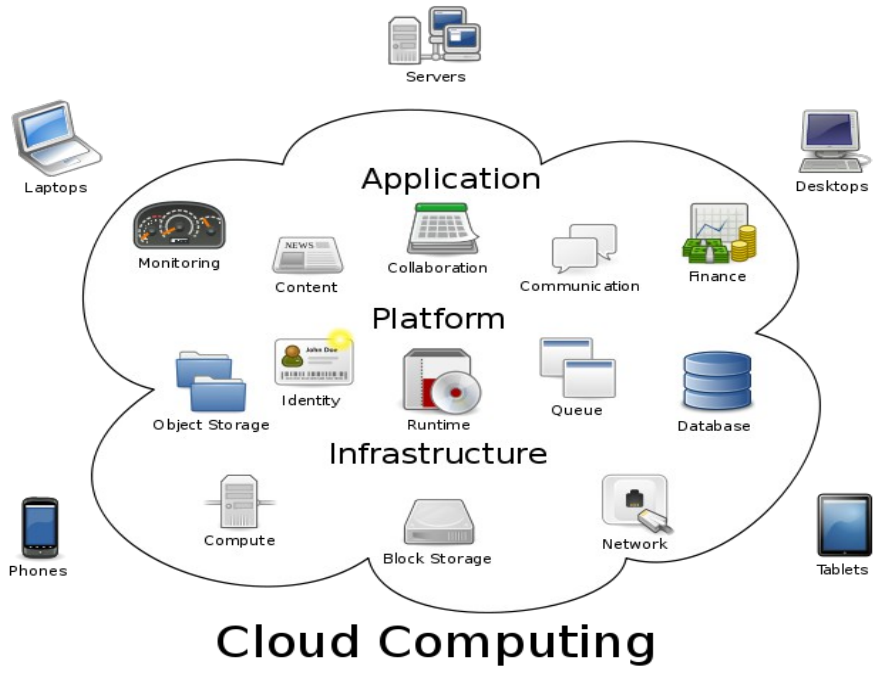
1. Definizioni

Una prima considerazione connessa alla nebulosità definitoria della nuvola è la constatazione che tutte le grandi aziende hardware e software offrono oggi *cloud computing*. Una semplice digitazione del termine in Internet sciorina una gamma di aziende quali HP, Telecom, Microsoft, INTEL, Cap Gemini, IBM, Aruba, Amazon, Accenture e via dicendo che si qualificano come elargitrici di servizi a nuvola. E, procedendo nella metafora, qualcuno spiega quali "gocce"/servizi si possono implementare.

Una definizione per "scemi" (*dummies*), dal sito per scemi (speriamo etimologici) informatici, sicuramente carenti di informazioni informatiche, ci informa che:

> "La 'nuvola' nel cloud computing si può definire come l'insieme di hardware, reti, memoria, servizi, interfacce che si combinano per rilasciare aspetti dell'elaborazione sotto forma di servizi. I servizi cloud includono il rilascio di software, infrastruttura e memoria su Internet (sia come componenti separate sia come piattaforma completa) sulla base delle richieste)" (http://www.dummies.com/how-to/content/what-is-cloud-computing.html).

Chiarissimo no? Ed eccone una rappresentazione grafica.



Il NIST americano, in "*The Future of Cloud Computing*", ne dà questa definizione:

"Il cloud computing è un ambiente di esecuzione elastico che consente l'accesso via rete e su richiesta ad un insieme condiviso di risorse di calcolo configurabili (ad esempio rete, server, dispositivi di memorizzazione, applicazioni e servizi) sotto forma di servizi a vari livelli di granularità. Tali servizi possono essere rapidamente richiesti, forniti e rilasciati con minimo sforzo gestionale da parte dell'utente e minima interazione con il fornitore."

Come è dato intendere, l'elasticità della nuvola si estende ai diversi dispositivi e terminali del sistema, moltiplicando la potenzialità dei servizi, pubblici e privati, ma aumentando contestualmente i rischi di sicurezza e *privacy.* Vedremo, fra poco, i "tipi"e i "modelli" di funzionamento della nuvola riassunti dalla grafica.

2. I vantaggi della nuvola

Veniamo, anzitutto, ai vantaggi del *cloud computing* che si possono riassumere nell'**elasticità** e nella **scalabilità** dei servizi offerti, nell'approvvigionamento **self-service** e nel de-approvvigionamento automatico, in **interfacce di applicazione** di programmazione, nella **fatturazione e nel controllo** dei servizi a consumo: insomma un supermercato/distributore di servizi globali, customizzabili,on line.

Altre definizioni spiegano che il *cloud computing* sposta tutte o alcune delle infrastrutture e delle operazioni IT di un'organizzazione, affidandole a qualcun altro (Chris Poelker, autore di *Storage Area Networks for Dummies*). Poelker, aggiunge che:

"il 'cloud computing' è la realizzazione dell'utility elaborativa per le masse , dove i servizi IT sono ora virtualizzati e forniti con architetture modulari create dai fornitori e dai venditori piuttosto che dagli utenti".

Questa espansione della definizione e i relativi vantaggi continuano a dirci ciò che il "cloud"è, come suggerisce qualcuno, ma non ciò che fa, specificamente. Ciò che possiamo intendere è che, analogamente a servizi per l'utenza normale quali la posta elettronica o l'hosting di un sito o l'uso di una piattaforma *social*, il "cloud" svolge servizi diversi, senza che l'utente debba comprare o installare software o hardware specifici. Si paga l'uso dei servizi ma non l'acquisto HW e SW degli stessi. La spesa IT, insomma, diventa solo una ***spesa operativa***. Questo lascia intendere, altresì, che il vantaggio del fornitore di piattaforme di *cloud computing* stia nell'offerta competitiva di servizi, ovvero nella qualità, nei costi proposti e nella quantità di acquisizione di clienti da parte del venditore degli stessi: un pò come i costi per la PEC o la firma digitale.

Una sottile filigrana di dubbio si insinua quando si considera che l'elaborazione di contenuti su piattaforme estranee richiede appunto la consegna a queste dei contenuti di informazione personale o di sistema. L'offerta di elaborazione o di memorizzazione di dati implica, in altri termini, il fatto che questi risiedano sulla piattaforma del fornitore. Il dubbio è ancor più consistente se a depositare informazioni e dati sono aziende o istituzioni, che probabilmente possiedono dati sensibili, per i quali il controllo di privatezza e sicurezza deve essere assoluto.

Reuven Cohen, fondatore di *Enomaly* a Toronto, in Canada, descrive il *cloud computing* come software Internetcentrico, appoggiato a multipiattaforme globali, multiproprietarie, multirete, scalabili.

Qui, diremmo, il vantaggio distributivo e di costi eccita il quesito circa la "multiproprietà". Si tratta di multiproprietà dei servizi di elaborazione offerti, ovvero di multiproprietà della piattaforma e dei suoi contenuti o solo della piattaforma o solo dei contenuti e di chi, fornitori e/o clienti? La scalabilità è un indubbio vantaggio ma la **modalità di gestione dei dati** (continuità e accessibilità

del servizio, soluzione di problemi, efficacia e utilità dell'elaborazione, *privacy* e sicurezza, ecc.) rimane un tema di primaria importanza e di non chiarissima definizione.

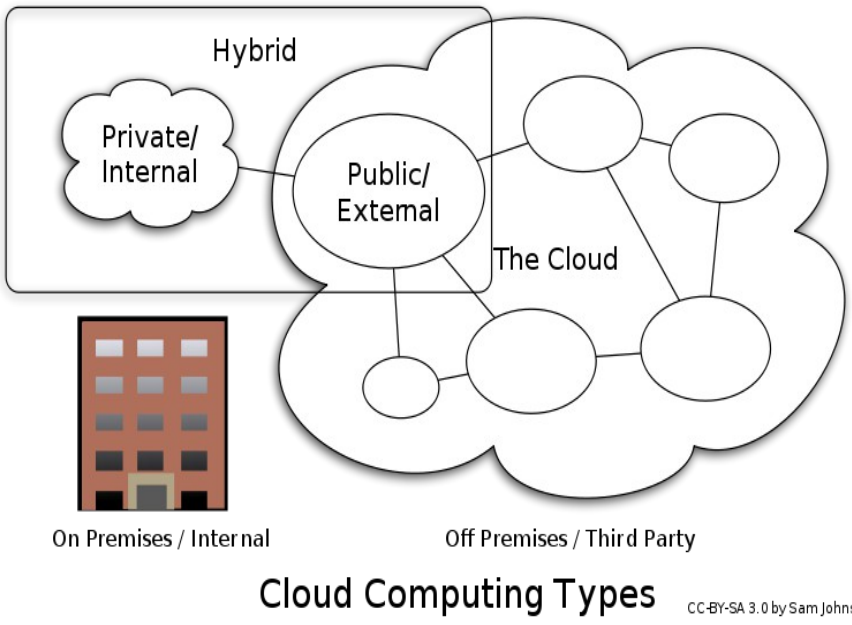
In ogni caso, le risorse onnipresenti disponibili nel "cloud", la fornitura semplice, immediata, su richiesta e il controllo altrettanto semplice, potenzialmente, e facile di tali risorse non può non apparire allettante e vantaggioso.

3. Le tipologie di "cloud"

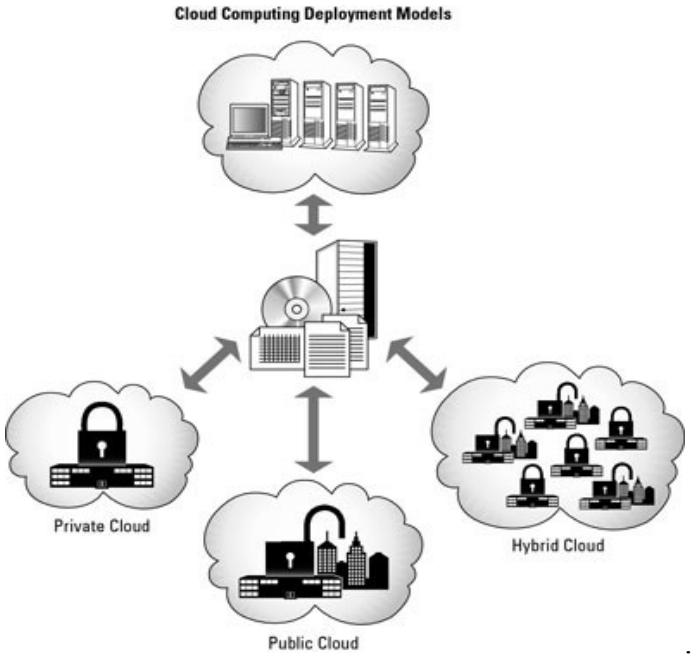
I tipi di "nuvola" offerte sono tre: pubbliche, private o ibride.

Come si vedrà, lo schema che segue rende l'idea che i servizi elaborativi e trasmissivi offerti e le informazioni depositate o accessibili per l'elaborazione possano essere del tutto sicure, chiuse, come nel modello privato; tutte aperte, come nel "cloud" pubblico; aperte e chiuse nel sistema ibrido.

A queste si possono aggiungere le "cloud di comunità" che possono condividere tra organizzazioni l'infrastruttura e i servizi.



Cloud Computing Types



In tutti i casi, a meno che l'Ente o l'Azienda fornitrice eroghi servizi a nuvola ai propri soggetti interni, si intende che i dati passano di controllo, come detto, ai fornitori/Aziende del supermercato digitale on line, la nuvola. In altri termini, la fruizione della nuvola coincide con un'estraneazione dei dati, in parte o del tutto, sia da parte del privato, sia dell'Azienda o dell'Istituzione e implica la necessaria garanzia di gestione della *privacy*, in particolare di dati sensibili, e di sicurezza della gestione dei medesimi da parte di attacchi esterni e usi illeciti o, anche, della continuità e regolarità dei servizi. E' come depositare i propri beni in una grande cassaforte cui possono accedere soggetti non proprietari ai quali è affidata altresì la combinazione d'accesso.

Si dirà che questo accade nelle cassette di sicurezza delle banche; ma nella fattispecie, i beni di cui trattiamo non sono fisici, sono immateriali, intangibili: sono conoscenza operativa e transattiva, in azione, movimento, anche traslazione, migrazione, riaggregazione.

L'allettamento rappresentato dall'accesso alle diverse tipologie di servizi offerti dal fornitore e dalle economie di scala pone pertanto agli Enti/ Aziende/soggetti pubblici e privati un importante quesito: come fidarsi del Grande Fratello tecnologico che, disponendo delle informazioni di sistema di molti soggetti, diventa potenzialmente il depositario/controllore di conoscenze e dati, sensibili all'origine o successivamente, se aggregati in forme nuove ovvero di una gamma di informazioni tipologicamente immensa e globale: informazioni economiche, sociali, finanziarie, culturali, ecc. La costituzione, in altri termini, di grandi *data centre* presso Aziende/piattaforme nuvola, che eroghino servizi a una pluralità di utenti, ad esempio alle Amministrazioni dello Stato, porrebbe il quesito relativo al tasso di apertura e disponibilità delle basi di dati delle Amministrazioni dello Stato e al potere combinatorio delle stesse nelle visioni di governo e di scelte istituzionali, sociali, economiche connesse, in ambito nazionale o, addirittura, mondiale. Non a caso, lo stesso dibattito sugli *open data*, ripropone la domanda strategica su chi si accaparrerà la fetta di "conoscenza" istituzionale maggiore e sul potenziale rischio di creare i nuovi mandarini del terzo millennio, ovvero i grandi gestori di servizi di conoscenza estraniati, esternati su piattaforme potenti e ricchissime di dati.

Come vedremo fra poco, il dibattito all'estero è da tempo avviato e rallenta decisioni definitive nell'e-government, che non siano accuratamente vagliate dal sistema Paese.

4. Il dibattito

   Vediamo di accostarci, per cominciare, al NIST (*National Institute of Standards and Technology*), organismo statunitense che elabora standard e linee guida tecnologiche per le Agenzie federali.

L'*Office of Management and Budget* ha imposto alle Agenzie federali di utilizzare un processo denominato programma di gestione del rischio federale e dell'autorizzazione, FedRAMP (*Federal Risk and Authorization Management Program*), per la valutazione e l'autorizzazione all'uso di prodotti e servizi "cloud".Il FedRAMP prevede una serie di specifiche di controlli di sicurezza per garantire la protezione negli ambienti *cloud*. Il programma Fed RAMP ha inoltre istituito un *board* centrale di alta dirigenza responsabile della definizione degli standard di accreditamento per i soggetti terzi che intendano offrire soluzioni "cloud". Lo stesso organismo controllerà i pacchetti autorizzativi e le autorizzazioni alle forniture, ferma restando la responsabilità finale nell'autorizzazione da parte dell'Agenzia federale (http://www.gsa.gov/portal/category/102371).

In ambito europeo l'ENISA, Agenzia dell'Unione europea per la rete e la sicurezza dell'informazione, opera per gli stati membri e le istituzioni offrendo consulenza, buone pratiche e raccomandazioni. In particolare ENISA si sta occupando del programma di rischio emergente e futuro. Nell'ambito del *cloud computing* che ENISA sostiene essere considerato strategico da molti governi europei, ENISA afferma di essere ampiamente coinvolta in richieste provenienti da agenzie europee che chiedono consigli sulla sicurezza relativa ai progetti di "cloud".
Considerando la tendenza ad aumentare il numero di *data centre* globalmente distribuiti si sottolinea che il fallimento di un singolo fornitore potrebbe compromettere un'intera economia nazionale. Ciò in connessione con l'Agenda europea che propone una strategia di *cloud computing* relato al government e alla scienza. L'iniziativa CAMM (Modello di maturità della sicurezza della nuvola) dovrebbe elaborare criteri per la sicurezza nei processi di *procurement* delle amministrazioni.

E in Italia, a quale punto è il dibattito?

L'Ufficio studi dell'Agenzia per le garanzie nelle telecomunicazioni sostiene che occorre:

• ponderare rischi e benefici dei servizi "cloud";
• verificare l'affidabilità del fornitore;
• privilegiare i servizi che favoriscono la portabilità dei dati;
• assicurarsi la disponibilità dei dati in caso di necessità;
•considerare il "*mirroring" / hot back up* – ovvero i dati sparsi su più server (*business continuity / disaster recovery*);
• selezionare i dati da inserire in cloud e quelli da tenere "in house";
• seguire i dati e dove risiedono / risiederanno fisicamente --*virtualized content ownership / data sovereignity*;
• chiare e trasparenti clausole contrattuali – QoS, SLA, i costi di trasferimento o di lock-in dei dati, gli standard e l'interoperabilità;
• tempi di persistenza /cancellazione dei dati nel cloud;
• tutela confidenzialità / sicurezza dei dati -- protezione dei dati personali;
• l'adeguata formazione del personale.

Nel citare la direttiva europea sugli obiettivi della policy e sui principi regolatori dei servizi ai cittadini (Policy objectives and regulatory principles , Directive 2002/21/EC as amended by Directive 2009/140/EC – Article 8), l'Ufficio studi dell'AgCom richiama l'art. 8 e altri articoli che da un lato promuovono il diritto a nuovi servizi digitali in Internet a favore dell'utente europeo, dall'altro invitano all'attenzione alla sicurezza e all'integrità delle reti.

In un recentissimo rapporto (maggio 2012) , Digit PA, in ordine alla normativa sugli appalti, afferma che :

"In considerazione dell'assenza di specifiche disposizioni riguardanti il cloud computing e di una sostanziale assenza di prassi operative al riguardo, risulta particolarmente interessante esplorare le possibili soluzioni che una PA potrebbe adottare per contrattualizzare un'iniziativa di cloud, utilizzando degli strumenti non specificamente pensati per tale tipologia di attività."

e suggerisce ipotesi contrattuali.

Sul tema "sicurezza" Digit PA non sembra avere dubbi:

"L'ultimo passaggio, quello della sicurezza, è evidentemente di estrema rilevanza in materia di tutela dei dati personali, e andrebbe considerato quale valore aggiunto del cloud anziché essere percepito come un elemento di debolezza di questa modalità di erogazione di servizi.
Occorre riconoscere che il punto è controverso ed è stato oggetto di vivace dibattito. **Pare tuttavia che lo sfavore manifestato quanto alla sicurezza dei dati in un contesto cloud sia dovuto soprattutto ad un sospetto iniziale, ma non abbia trovato espressione in oggettive e argomentate ragioni. Al contrario, l'analisi obiettiva dei requisiti necessari ad assicurare un elevato livello di sicurezza dei dati spinge a conclusioni del tutto diverse (** grassetto nostro**).** In effetti, va considerato che la sicurezza informatica ha un costo rilevante e richiede un investimento dedicato. Dipende da una serie di fattori strettamente materiali, tutti alla portata della "massa critica" di un cloud provider ma non necessariamente sostenibili da soggetti come le PA, che devono destinare in via principale ad altre finalità le loro risorse. La sicurezza informatica richiede una notevole dotazione di tecnologie, la predisposizione di un'organizzazione dei sistemi e di personale ad hoc, l'utilizzo di protocolli sempre aggiornati, la formazione costante dei tecnici e la capacità di pronta reazione alle 'falle' informatiche di volta in volta emergenti."

In verità, la sola preoccupazione di sicurezza qui esposta sembrerebbe riguardare i dati relativi al cittadino, prescindendo, dunque da informazioni economiche, sociali, finanziarie che, certamente, non possono che turbare, nella prospettiva di usi irrituali rispetto a quelli tradizionali, come dimostrano, ad esempio, le attuali bufere finanziarie internazionali che sempre di informazioni si nutrono.

Appare dunque sottostimato questo aspetto e riduttive le conclusioni per le quali:

"Il problema sicurezza perciò va affrontato non tanto in termini di natura tecnico-informatica, dove il cloud risulta significativamente vantaggioso, quanto piuttosto in termini negoziali-contrattuali, strettamente legati **alla forza dei buyer di imporre al provider le "regole d'ingaggio", livelli di servizio e di rispetto della disciplina sulla tutela dei dati personali ritenuti soddisfacenti**, nonché di stabilire con precisione la responsabilità contrattuale di quest'ultimo (e degli ulteriori eventuali soggetti coinvolti nell'erogazione dei servizi in modalità cloud) in caso di violazione.
Sul punto potrebbe essere opportuno lo studio di **eventuali linee guida di settore che traccino le garanzie minime** (grassetto nostro) in presenza delle quali la PA possa aderire al cloud. Ciò avrebbe effetti positivi non solo per entrambe le parti coinvolte, ma stimolerebbe lo sviluppo di best practice cloud per la PA perché: chiarirebbe i requisiti minimi che devono essere tenuti in considerazione dai provider nel proporre un'offerta cloud per la PA; potenzierebbe la forza negoziale della PA al fine di ottenere servizi sempre più rispondenti alle proprie esigenze; stimolerebbe la concorrenza dei provider al fine di fornire soluzioni volte alla massima soddisfazione anche dei requisiti legali necessari al fine di erogare i propri servizi alla PA."

Ma sul tema, osserviamo che non si tratta dei soli dati personali, questione sulla quale il Garante della privacy è recentemente intervenuto, e per i quali , in ogni caso, la soluzione a difesa della privacy non è certo il *backup* degli stessi. Qui si tratta di un controllo decisivo su cosa può essere

definito pubblico e cosa non lo è e, soprattutto, dell'impossibilità di impedire un uso illecito o dannoso dei dati stessi, essendo gli stessi fuori del controllo statuale amministrativo del cliente.

E' evidente che la necessità di mediare tra il mercato e le istituzioni conduce a ipotesi contraddittorie e a valutazioni semplificatorie che, in ogni caso, dovrebbero invece suggerire cautela.

Come si vede, il lavoro è *in progress* ma le soluzioni ancora mancano. Nel frattempo che fare? Cedere subito al fascino della nuvola o verificare gli ambiti di sicurezza obbligatori per i dati; affidarsi alle promesse di buona condotta dei fornitori o pretendere e verificare sperimentalmente i rischi? Discutere gli aspetti legali e contrattuali o immergersi nell'atmosfera ovattata delle incertezze diffuse?
E di quali insicurezze e rischi stiamo parlando?

5. La sicurezza e la privacy

Nella valutazione dei rischi si colloca, primo fra tutti, la **sicurezza.** Da un lato si afferma che la sicurezza può addirittura aumentare dal punto di vista della centralizzazione dei dati ma può altresì comportare la **perdita di controllo di dati sensibili e la mancanza di sicurezza di nuclei di dati.** Si comprende, pertanto, perché la nuvola sia più allettante per installazioni private che non nei sistemi multiproprietari dove la sicurezza distribuita diventa più complessa. Sui temi della **sicurezza** e della **privatezza** riassumiamo i sei aspetti principali:

La **gestione dell'identità per l'accesso all'informazione**. Questa può essere lasciata al fornitore, all'interno della piattaforma, o al cliente che la gestisce come crede. E' un tema già affrontato nella gestione fisica locale.
La **sicurezza fisica della macchina e del personale**. Il fornitore garantisce che le macchine sono adeguatamente sicure e che l'accesso ai dati è non solo limitato ma anche documentato. E' un primo aspetto nodale nella scelta del fornitore/venditore.
La **disponibilità del servizio**. Il fornitore assicura i clienti che avranno accesso regolare ai loro dati e alle loro applicazioni. In questo caso si pone il problema dell'affidabilità tecnologica dell'offerta.
La **sicurezza delle applicazioni**. I fornitori garantiscono attraverso test e procedure specifiche le applicazioni esterne. Altro aspetto da valutare e testare.
La **privacy**. I fornitori garantiscono non solo il mascheramento dei dati e l'accesso ai soli utenti autorizzati ma anche la protezione delle identità e delle credenziali digitali.
La capacità "**investigativa" e la legalità.** Il fornitore e il cliente devono saper e poter individuare l'attività lecita rispetto a quella illecita.
La **crittografazione.** E' essenziale la codifica protettiva dei dati e delle informazioni.

A ciò si aggiungano, infine, i temi legali inerenti contratti, *disclosure*, ecc.
(http://www.cloudsecurityalliance.org/guidance/csaguide.v3.)

Soluzioni sicure possibili, in essere, sono potenzialmente già presenti, laddove i soggetti che gestiscono la nuvola, già possiedano i dati. E' il caso dell'Anagrafe tributaria o della Banca d'Italia che possono convertirsi in grandi gestori/distributori per soggetti i cui dati siano già noti. Ma ciò che manca ad essi, sono i dati di cui non sono in possesso e che potrebbero essere convogliati nei *data centre* di servizi, per distribuire o gestire i servizi stessi: grandi basi di dati, interfacciamento tra amministrazioni, programmi elaborativi inediti. Dunque, grandi opportunità e grandi quesiti.

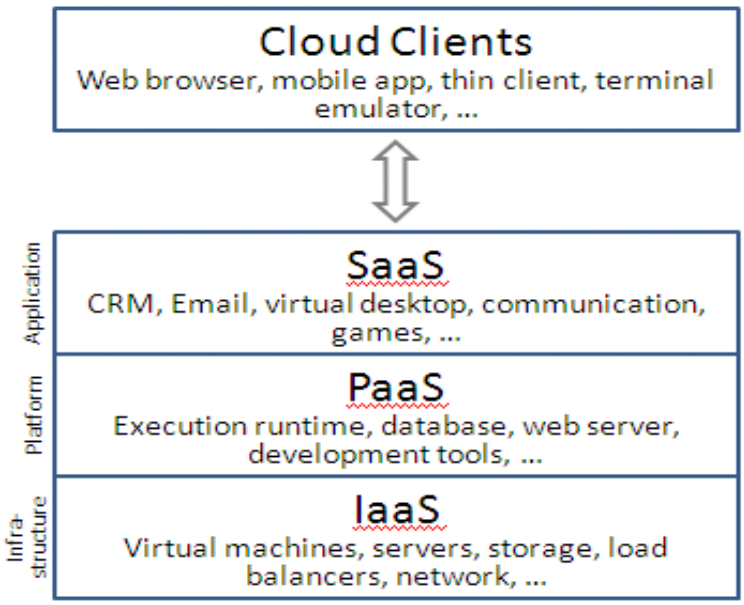
Veniamo, ora, alle tipologie di modelli di "cloud".

6. I modelli di *cloud computing* e i criteri da verificare

Il modello **Iaas**, infrastruttura come servizio, offre risorse di **memoria** ed **elaborazione: macchine virtuali, server, firewall, reti locali** ed eventualmente **reti private dedicate** o **Internet per le reti geografiche.** Dunque, informazione e dati depositati presso il fornitore in grandi *data centre* ai quali accedono i clienti. Applicazioni e servizi sono svolti dai clienti che pagano solo l'infrastruttura.

Il modello **PaaS**, piattaforma come servizio, offre strumenti per sviluppare applicazioni sulla piattaforma elaborativa: servizi di **accesso ai dati**, servizi di **basi di dati**, servizi di **fatturazione.** Anche in questo caso, le applicazioni non potrebbero evitare l'esternalità dei dati che vengono elaborati sulla piattaforma.

Il modello **SaaS**, software come servizio, infine, implica la possibilità di ospitare del software. Anche in questo caso, il software si appoggia su una piattaforma che ospita dati.



Sotto un profilo generale, i tratti specifici che la letteratura sull'argomento propone di valutare sono i seguenti.

- La **sicurezza della nuvola.** E' la stessa sicurezza nelle soluzioni attuali con l'aggiunta dell'applicazione delle regole già evidenziate.

- La **gestibilità della nuvola.** E' la capacità forte di gestione dei servizi, sia *in loco* sia nella nuvola.

  Questo, osserviamo, è forse il tema più preoccupante nel nostro contesto. Gestire servizi informatici richiede anzitutto un'analisi e una capacità progettuale informatica forte in

un'azienda come in un'amministrazione. Occorre cioè progettare i servizi da gestire mediante i servizi della nuvola. E', ad esempio, evidente che nessuna nuvola consentirà di gestire un procedimento amministrativo o di costruire una base di dati degna del nome, senza un'adeguata progettazione del servizio gestionale informatico atteso. In altri termini, come già spiegato per l'impiego di CMS, i servizi offerti dalla nuvola devono essere comunque progettati, riprogettati e sviluppati. E qui torniamo al tasso di insufficienza attualmente riscontrabile nella gestione informatica delle nostre amministrazioni, pur con le debite distinzioni d'ambito e di soluzioni. Qualità e quantità dei servizi a nuvola da usare vanno confrontati e sviluppati, caso per caso, con soluzioni architetturali dell'informazione innovative.

- Gli **standard della nuvola.** Gli standard adottati da una nuvola, leggasi fornitore, devono essere interoperabili con le altre nuvole di sistema. Nelle amministrazioni dello stato, ciò richiederà una forte intesa tra fornitori di nuvole per i *data centre* ipotizzati, una portabilità da un venditore/fornitore ad un altro, per evitare la diaspora nell'interfunzionalità dei sistemi, ad esempio dal centrale al locale. Ma siamo pronti a questo cambio di marcia? E' il tema perenne del livello di competenza informatica nelle amministrazioni e del rapporto fornitore/cliente.

- La **governance e le regole della nuvola.** Se la governance ha a che fare con la responsabilità dei processi e delle policy adottate, nel caso della nuvola tale responsabilità è raddoppiata e complicata dal fatto che il controllo dei processi è anche esterno e quindi non direttamente controllabile. Nella governance della nuvola vanno, dunque, incluse le regole di sicurezza e privacy e la valutazione del successo ovvero il reale perseguimento degli obiettivi attesi.

- La **gestione dei dati**. Nella nuvola, oltre alla sicurezza e alla privacy, la gestione dei dati deve occuparsi del rischio di trasferimento e di migrazione degli stessi da un punto A a un punto B.sulla nuvola o tra nuvole diverse.

Non siamo certi, a questo punto, di aver problematizzato il discorso ai fini di una meditata valutazione delle scelte in essere o in discussione, ad esempio nella cabina di regia del governo in materia di Agenda digitale. Sono di questo tipo i *data centre* di cui si parla? Se sì, per quali attività gestionali? Per quali finalità?Per quali fornitori? Con quale estensione e quale granzia di privacy e di sicurezza? Con quali regole, nazionali o extranazionali se le piattaforme fisiche del fornitore risiedono all'estero?

Al di qua o al di là della nuvola, sarebbe tempo di vedere progetti concreti di gestione di procedimenti e servizi in chiave tecnologica e di disporre di basi di dati, siti e portali razionali, interattivi, realmente partecipativi. A quando e a chi la responsabilità? Avremo tanta nuvola e poco arrosto? Spenderemo meno per uguali servizi o per non avere affatto servizi? Chi si assumerà la responsabilità di queste decisioni e di questi processi?

Un momento di riflessione, per favore.