DigitPA

RACCOMANDAZIONI E PROPOSTE SULL'UTILIZZO DEL CLOUD COMPUTING NELLA PUBBLICA AMMINISTRAZIONE

Versione 1.7 del 14 maggio 2012

Sommario

PREMESSA

CONTESTO

Con riferimento ai propri compiti istituzionali, in particolari alle funzioni di proposta per sistemi ICT innovativi e, in prospettiva, di interventi e progetti di innovazione, DigitPA ha ritenuto di emettere un documento contenente raccomandazioni e proposte per l'adozione del paradigma cloud computing nella pubblica amministrazione. Allo scopo, anche alla luce delle risultanze del convegno che DigitPA aveva organizzato nell'ottobre 2010, è stato istituito un gruppo di lavoro per raccogliere i contributi e le opinioni di una varietà di *stakeholder* comprendente esperti, amministrazioni, aziende e altri organismi attivi nel settore. Il presente testo di raccomandazioni e proposte è il risultato di una elaborazione autonoma di DigitPA condotta sul materiale prodotto dal gruppo di lavoro.

Nell'elaborazione di questo documento si è tenuto conto di una serie di rapporti della Commissione europea, di ENISA (*European Network and Information Security Agency*) e di altre organizzazioni internazionali, di studi accademici, di rapporti di società di consulenza e di una serie nutrita di studi e progetti finanziati dai programmi FP7 (*7th Framework Programme for Research*), CIP – ICT PSP (*Competitiveness and Innovation Framework Programme – ICT Policy Support Programme*) e ISA (*Interoperability Solutions for European Public Administrations*). Di particolare rilievo da un punto di vista strategico le indicazioni provenienti dall'*eGovernment Action Plan 2011-2015* e dalla *Digital Agenda for Europe* e quelle attese dalla *European Cloud Computing Strategy* e dalla *European Cloud Partnership*.

OBIETTIVI

L'obiettivo di questo documento di raccomandazioni e proposte è duplice. Da una parte raccoglie considerazioni e proposte rilevanti ai fini dell'adozione del cloud computing da parte della pubblica amministrazione in Italia. Dall'altra si promette di offrire strumenti utili a questo scopo privilegiando un approccio che oltre a proporsi con finalità di razionalizzazione e di risparmio miri anche a promuovere un'organizzazione innovativa dei servizi pubblici online che le soluzioni tecnologiche e operative del cloud rendono possibile. Coerentemente, nel documento vengono solo marginalmente affrontate alcune problematiche più tecniche connesse alla naturale evoluzione tecnologica dei data center, anche perché a tale tematica sarà dedicato un apposito documento che terrà conto di quanto emerso nel corso delle attività di valutazione, monitoraggio e coordinamento svolte da DigitPA.

Si osserva infine che l'evoluzione della società digitale e la normativa (ad esempio [CAD05]) pongono di fronte ad adempimenti identici sia un grande ministero che un piccolo comune, che pure dispongono di risorse e di competenze non confrontabili. Il documento contiene indicazioni differenziate utilizzabili da entrambi questi attori.

Infine, anche attraverso questo documento DigitPA è impegnata a contribuire all'elaborazione e all'implementazione delle iniziative europee, con riferimento specifico alla messa in atto della strategia europea in sede nazionale attraverso l'Agenda Digitale Italiana.

DESTINATARI

L'adozione di soluzioni di tipo cloud presuppone l'incontro tra domanda e offerta che, almeno per quanto riguarda la pubblica amministrazione, si ritiene incompleto. Non si tratta soltanto di esplicitare requisiti puntuali (ad esempio in materia di privacy o di tracciabilità dei dati) ma soprattutto di definire direzioni e scenari tecnologici che risultino integrati con le correnti politiche di eGovernment.

Per questo motivo, i destinatari di questo documento includono sia i decisori che i gestori, indicando con queste espressioni tutti i soggetti in grado di influenzare da un lato la definizione delle politiche ICT e dall'altro la loro implementazione a livello centrale e locale.

Prossimi passi

Per accompagnare le pubbliche amministrazioni nel percorso di adozione del cloud computing, DigitPA svolgerà nei loro confronti attività di promozione, di sostegno e di monitoraggio in linea con le proprie funzioni istituzionali.

Le attività di promozione comprendono azioni di diffusione della conoscenza, di formazione e di scambio di buone prassi. Questo documento costituisce la base di tali attività e contiene alcuni primi strumenti utili per il suo svolgimento.

La fase di sostegno richiede invece strumenti, qui solo delineati, necessari alle amministrazioni per condurre l'analisi dei requisiti, dell'attrattività delle soluzioni cloud e della loro fattibilità dai diversi punti di vista (logistico, amministrativo, regolatorio, tecnologico). Tali strumenti comprenderanno modelli e criteri economici, standard tecnici e regole condivise. La realizzazione di sperimentazioni e di progetti pilota potrà fornire dati empirici e indicazioni a sostegno delle diverse opzioni operative.

Infine, le azioni di monitoraggio e di verifica saranno svolte da DigitPA attraverso gli strumenti dei pareri rilasciati alle amministrazioni sugli interventi e contratti relativi all'acquisizione di beni e servizi informatici.

Struttura del documento

Il documento è articolato in tre capitoli introduttivi che conducono al capitolo finale, il quarto, contenente le raccomandazioni e proposte.

Nel primo capitolo il paradigma cloud computing viene introdotto da un punto di vista prevalentemente tecnologico facendo ricorso a definizioni largamente diffuse e accettate. Nel secondo vengono esaminati le opportunità e i rischi dell'adozione dei servizi cloud nei diversi ambiti relativi all'economia, alla normativa, alla *privacy*, alla sicurezza e alle infrastrutture ICT. Il terzo capitolo cerca di individuare i principali fattori di successo che emergono dall'analisi contenuta nei capitoli precedenti. Infine, il quarto capitolo elenca in forma sintetica una serie di raccomandazioni e proposte.

Si avverte che, in considerazione della loro forte correlazione in questo specifico ambito, si è preferito raggruppare le tematiche di privacy con quelle di sicurezza anziché con quelle giuridiche.

Ringraziamenti

Il presente documento è stato curato da Daniele Tatti e Aldo Liso (DigitPA) con il prezioso contributo di Daniele Catteddu (ENISA e, successivamente, CSA) per gli aspetti legati alla sicurezza e per il sostegno in tutte le fasi del lavoro, Paolo Mori (CNR – IIT) per l'introduzione al cloud computing, Paolo Balboni (partner, ICT Legal Consulting) per gli aspetti relativi alla privacy e Massimo Macchia (DigitPA) per gli aspetti contrattuali.

Si ringraziano i rappresentanti delle amministrazioni, delle aziende e di altri organismi e tutti gli esperti che hanno partecipato a titolo volontario al gruppo di lavoro "Cloud computing e pubblica amministrazione". L'ampia partecipazione delle aziende associate ad Assinform è stata resa possibile da Giuseppe Neri.

Al gruppo di lavoro hanno partecipato rappresentanti di Accenture, Almaviva Italia, Almaviva TSF, AMD, Assinform, Banca d'Italia, BT Italia, Business-e, Cisco, Compuware, CONSIP, CSI Piemonte, Dell, EMC, ENISA, Fujitsu Technology

Solutions, Google, Hitachi Data Systems, IBM, CNR – IIT, INPS, Insiel, Intel, LUISS – CeRSI, Microsoft, Netapp, Oracle, PA Digitale, Par-Tec/Babel, Regione Marche, Regione Piemonte, Regione Toscana, Regione Veneto, SAP Italia, Selex Elsag, Siemens, SIRTI, Sogei, Studio legale Belisario, Telecom Italia, ULSS 8 – Asolo, Università del Piemonte Orientale, Università di Roma "La Sapienza", Università di Torino, VMware. Hanno anche collaborato a titolo personale Ernesto Belisario (Studio Ernesto Belisario), Cosimo Comella (Autorità garante per la protezione dei dati) e Flavia Marzano (Stati Generali dell'Innovazione).

La loro partecipazione ci ha permesso di condividere le aspettative legate al cloud computing ma anche di acquisire concrete esperienze.

1. CHE COS'È IL CLOUD COMPUTING: TECNOLOGIE E PRESTAZIONI

Il cloud computing è un nuovo approccio per la fornitura di risorse IT (capacità computazionale, spazio di memorizzazione o anche software) sotto forma di servizi accessibili via rete. Esistono varie definizioni di cloud nella letteratura scientifica. Di seguito utilizziamo come riferimento una definizione che riassume quelle proposte dal *National Institute of Standards and Technology* (NIST) [NIST11] e da un gruppo di esperti riuniti dalla Comunità Europea nel report "*The Future of Cloud Computing*" [EC10]:

> "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."

Molte altre definizioni per il cloud computing sono disponibili in letteratura scientifica, che cercano di catturare gli aspetti essenziali del cloud computing. In [VAQ09] vengono riportate molte altre definizioni, dalle quali gli autori cercano di evincere le caratteristiche principali del cloud. Altre definizioni interessanti sono quelle rilasciate da ERCIM in [ERC10], da SUN Microsystems [SUN09], e quelle riportate in [HOE10].

La definizione del NIST individua cinque caratteristiche principali per il cloud:

1. **Self-service su richiesta**: un cliente può unilateralmente richiedere nei vincoli fissati dal contratto risorse computazionali, come tempo macchina, risorse di memorizzazione o altro, quando necessario per svolgere i suoi task, senza richiedere un intervento umano dei fornitori dei servizi stessi.

2. **Accesso a banda larga**: le risorse sono raggiungibili tramite la rete, la cui banda deve essere adeguata all'uso specifico richiesto, e vengono accedute con meccanismi che ne permettono l'uso con piattaforme client diversificate ed eterogenee sia leggere che complesse (ad esempio telefoni cellulari, computer portatili, o computer palmari).

3. **Risorse comuni**: le risorse di calcolo del fornitore vengono organizzate per servire più clienti, utilizzando il modello multi-tenant, in cui le risorse fisiche e virtuali sono assegnate dinamicamente a seconda della richiesta dei clienti. Le risorse offerte sono indipendenti dalla loro locazione fisica, ovvero il cliente generalmente non ha né il controllo né la conoscenza dell'esatta locazione fisica delle risorse a lui fornite. Tuttavia, il fornitore potrebbe permettere all'utente di specificare dei vincoli sulla locazione delle risorse a lui assegnate in termini di area geografica, Paese o anche singolo data center. Esempi di risorse sono: risorse di memorizzazione, di calcolo, di rete e macchine virtuali.

4. **Elasticità**: le risorse possono essere fornite rapidamente ed elasticamente, ed in alcuni casi anche automaticamente, per incrementare velocemente la capacità computazionale, ed allo stesso modo possono essere rapidamente rilasciate per decrementare la capacità computazionale. Dal punto di vista dell'utente le risorse disponibili appaiono illimitate, e possono essere richieste in qualsiasi quantità ed in qualsiasi momento.

5. **Servizi monitorati**: i sistemi cloud controllano ed ottimizzano automaticamente l'utilizzo delle risorse, sfruttando la capacità di misurarne l'utilizzo delle risorse al livello necessario per il tipo di servizio (ad esempio servizi di memorizzazione, di calcolo, banda di comunicazione, ed account utente attivi). Il monitoraggio dell'utilizzo dei servizi è molto importante per permettere al fornitore di reagire ad eventuali picchi di richiesta

allo scopo di garantire al cliente la Qualità del Servizio promessa. L'utilizzo delle risorse può essere monitorato e riportato trasparentemente sia per il fornitore che per il cliente.

Altre proprietà caratterizzano i sistemi cloud computing. Tra queste, forse la più nota è la virtualizzazione, un insieme di tecnologie che permette di condividere i server e lo storage, di aumentarne radicalmente il tasso di utilizzo e di spostare facilmente le applicazioni da un server fisico ad un altro.

Un'ulteriore caratteristica del cloud computing è il pagamento in base all'utilizzo dei servizi. Infatti, l'utente può sfruttare i servizi cloud su richiesta, scegliendo il fornitore ed i servizi che ritiene opportuno a seconda delle proprie necessità, e può richiedere l'utilizzo delle risorse solo quando necessarie e solo per il tempo necessario. L'utente verrà poi addebitato dai fornitori di servizi solamente in base all'effettivo sfruttamento delle risorse stesse. Questa caratteristica permette all'utente un notevole risparmio sulle risorse IT, in quanto può ridurre la quantità di risorse elaborative presenti presso le sue strutture e conseguentemente il personale per la loro gestione, trasferendo al fornitore di servizi il rischio di inutilizzo delle stesse.

Come vedremo nel seguito, i servizi cloud possono essere di vario genere, a seconda del tipo di servizio offerto e della responsabilità di fornitura assunta che possono essere limitate alla messa a disposizione delle risorse o arrivare fino alla prestazione finale cui la soluzione ICT mira. Tali servizi possono essere implementati utilizzando risorse comuni offerte da un fornitore di servizi ai suoi utenti, oppure risorse dedicate ad un certo utente, fornite dall'utente stesso o da un fornitore esterno. L'utente, a seconda del problema che deve risolvere, sceglierà il tipo di servizio ed il fornitore più idoneo.

1.1 Modelli di servizio

Il servizi offerti dal cloud possono essere classificati in tre modelli principali, a seconda del livello al quale sono collocati, a partire dal livello hardware fino al livello applicativo. In particolare, partendo dal livello più basso, sono stati definiti tre modelli principali: *Infrastructure as a Service*, *Platform as a Service* e *Software as a Service*.

Infrastructure as a Service (IaaS)

Il modello di servizio *Infrastructure as a Service* prevede che il servizio offerto consista in una infrastruttura con capacità computazionale, di memorizzazione, e di rete, sulla quale l'utente possa installare ed eseguire il software a lui necessario, dal sistema operativo alle applicazioni. Nel caso di servizio computazionale, l'utente può richiedere al fornitore di servizi un insieme di macchine virtuali, sulle quali può installare (o richiedere che venga installato direttamente dal fornitore stesso) i sistemi operativi ed i software necessari a risolvere il suo problema. L'utente può richiedere che le macchine virtuali siano connesse tra di loro da una rete virtuale. Le macchini virtuali sono raggiungibili per la loro gestione ed utilizzo tramite l'interfaccia offerta dal fornitore del servizio. Una volta che le macchine virtuali sono state assegnate all'utente, egli può richiederne delle nuove o rilasciarne alcune, in base alle sue esigenze.

Nel caso di servizio di memorizzazione, invece, l'utente può richiedere uno spazio di memorizzazione per caricarvi i suoi dati e, successivamente, può aumentarlo o ridurlo a seconda delle sue esigenze.

Un esempio di fornitore di servizi IaaS di tipo computazionale è Amazon Elastic Compute Cloud (EC2) [AMA10], che tramite una interfaccia web permette di selezionare una immagine per le proprie macchine virtuali tra quelle disponibili (Amazon Machine Image, AMI) oppure di crearne una personalizzata e di avviarle e gestirle durante la loro esecuzione.

Anche Microsoft fornisce servizi cloud di tipo IaaS, tramite la piattaforma denominata Windows Azure Compute, che consente di eseguire immagini personalizzate di macchine virtuali con sistema operativo Windows Server 2008 R2.

Inoltre, sia Amazon che Microsoft sono esempi di fornitori di servizi IaaS di memorizzazione. Amazon fornisce il servizio Amazon Simple Storage Service (S3) che permette tramite una semplice interfaccia web service di memorizzare dati e di

accedervi da qualsiasi locazione ed in qualsiasi momento. Microsoft, invece, fornisce i servizi SQL Azure Database e Windows Azure Storage, che implementano un data base scalabile a disponibilità elevata basato sulle tecnologie SQL, ed un servizio di archiviazione protetto, scalabile, facilmente accessibile e duraturo.

PLATFORM AS A SERVICE (PAAS)

Il modello di servizio *Platform as a Service* prevede che il fornitore del servizio metta a disposizione dell'utente una interfaccia di programmazione (API) con la quale l'utente può scrivere applicazioni che interagiscono con il servizio. Le specifiche funzionalità offerte dalla API dipendono dal servizio offerto, e la loro esecuzione viene assicurata dal fornitore del servizio. Il fornitore può mettere a disposizione dell'utente anche un ambiente di sviluppo (e di testing) per le applicazioni che sfruttano le sue API.

Un esempio di servizio cloud di tipo PaaS è costituito da Windows Azure Compute, che permette di utilizzare il framework .NET per sviluppare applicazioni. Poiché utilizza IIS7, è anche possibile gestire applicazioni sviluppate utilizzando ASP.NET, Windows Communication Foundation (WCF) o altre tecnologie Web. Inoltre, supporta anche linguaggi quali PHP e Java.

SOFTWARE AS A SERVICE (SAAS)

Il modello di servizio *Software as a Service* prevede che il servizio offerto sia un'applicazione software che può essere utilizzata su richiesta. In questo caso, il fornitore del servizio installa l'applicazione nei propri data center, e fornisce agli utenti una interfaccia per utilizzarla, come ad esempio una interfaccia web. In alcuni casi, i servizi software potrebbero essere implementati dal loro fornitore usando altri servizi cloud a livello inferiore, cioè di tipo PaaS o IaaS.

Un esempio di servizi cloud di tipo software è costituito da Google Apps, che fornisce tramite interfaccia web un insieme di applicazioni per ufficio, come posta elettronica, videoscrittura, foglio di calcolo e calendario.

1.2 MODELLI DI DISPIEGAMENTO

Il modello di dispiegamento dei servizi cloud riguarda i data center in cui sono installati tali servizi. Infatti, i servizi possono essere installati nei data center di un fornitore che li rende accessibili a tutti gli utenti, nei data center degli utenti stessi, o su macchine riservate situate però in data center di fornitori pubblici, come descritto in seguito.

PUBLIC CLOUD

I servizi cloud pubblici sono offerti da fornitori che mettono a disposizione dei propri utenti/clienti la potenza di calcolo e/o di memorizzazione dei loro data center. Il tipo di servizi cloud che vengono offerti dal fornitore (IaaS, PaaS, SaaS) dipende dalla politica del fornitore stesso, così come il prezzo e la tariffazione.

Uno dei maggiori vantaggi del cloud pubblico per il cliente consiste nel fatto che egli può richiedere l'utilizzo dei servizi cloud di cui necessita nel momento in cui effettivamente ne ha bisogno, e solo per il tempo che gli sono necessari. In questo modo, il cliente può ridurre gli investimenti in infrastrutture IT e ottimizzare l'utilizzo delle risorse interne, perché può risolvere i picchi di calcolo periodici o imprevisti richiedendo l'utilizzo di servizi cloud quando essi si verificano.

Un lato negativo, invece, è che il cliente non ha il completo controllo dei suoi dati e dei suoi processi quando essi vengono gestiti dai servizi cloud pubblici. Infatti, tipicamente il fornitore non informa il cliente su dove risiedono le macchine su cui vengono processati e memorizzati i suoi dati, su dove vengono eseguite le sue macchine virtuali, o dove venga eseguito il software che il cliente stesso sta utilizzando. Inoltre, per quanto riguarda la sicurezza dei suoi dati, il cliente non può definire una propria politica di sicurezza, ma deve accettare quella dichiarata dal fornitore, e deve fidarsi del fornitore stesso, che effettivamente applichi le misure di sicurezza che ha dichiarato.

In questi ultimi anni c'è stata una notevole crescita nell'offerta di servizi cloud pubblici. Alcuni esempi di cloud pubblici sono Amazon, che fornisce sia servizi di tipo IaaS (Amazon EC2) che di Storage (Amazon S3), oppure Google App che fornisce servizi software (SaaS), come GMail, Google Docs oppure Google Calendar.

PRIVATE CLOUD

Un cloud privato viene installato dall'utente nel suo data center per suo utilizzo esclusivo. Il principale vantaggio di un cloud privato è che i servizi vengono forniti da elaboratori che si trovano nel dominio dell'utente, e quindi l'utente ha il pieno controllo delle macchine sulle quali vengono conservati i dati e vengono eseguiti i suoi processi. In particolare, l'utente può applicare su queste macchine le politiche di sicurezza che ritiene più opportune per la protezione dei suoi dati.

In alcuni casi, un cloud privato può essere installato da una grande azienda, o da un ente pubblico, che dispone di uno o più data center propri, per offrire servizi cloud alle varie divisioni dell'azienda stessa. In questo caso la stessa entità agisce sia da fornitore che da utente dei servizi cloud.

Un altro scenario possibile è invece quello in cui l'utente installa il proprio cloud privato nel data center di un terzo soggetto (tipicamente un fornitore di servizi cloud), in cui dispone di macchine dedicate. In questo caso, l'utente ha il controllo delle macchine anche se non risiedono nel suo dominio, e quindi può configurarle secondo le proprie necessità.

Per installare un cloud privato, sono attualmente disponibili diversi strumenti software, come ad esempio Eucalyptus, OpenNebula o Apache Tashi.

COMMUNITY CLOUD

Nel Community cloud l'infrastruttura su cui sono installati i servizi cloud è condivisa da un insieme di soggetti, aziende, organizzazioni, ecc, che condividono uno scopo comune e che hanno le stesse esigenze, come ad esempio potrebbero essere i vari soggetti della pubblica amministrazione. L'infrastruttura può essere gestita dalla comunità stessa, oppure da un fornitore di servizi esterno.

HYBRID CLOUD

Il cloud Ibrido è una combinazione del modello pubblico e di quello privato, ovvero è un modello in cui l'utente utilizza risorse sia del suo cloud privato che di un cloud pubblico. Il cloud Ibrido può essere utilizzato con successo in vari casi.

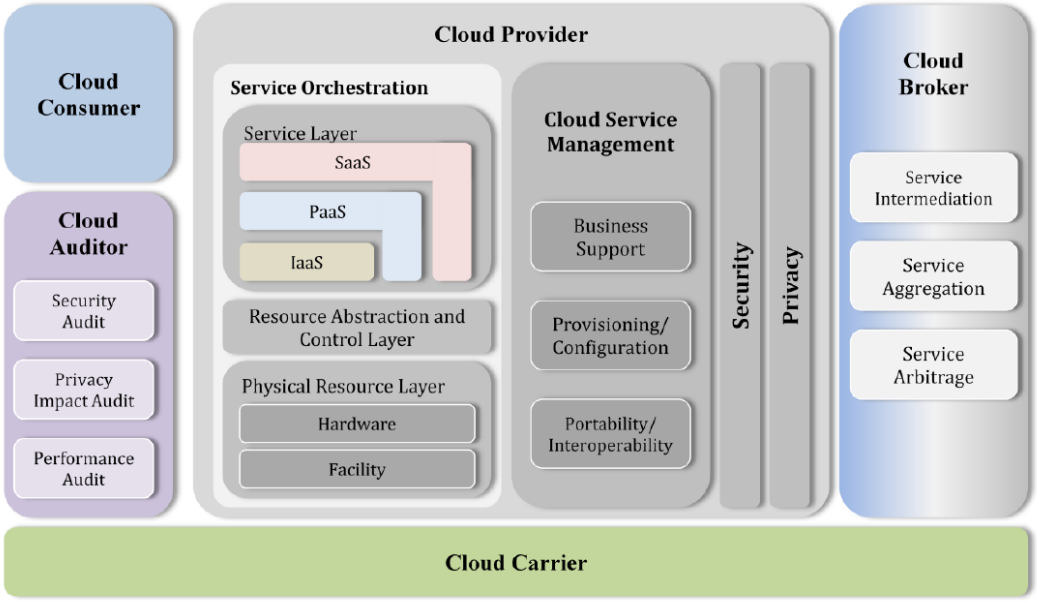
Ad esempio, un utente che dispone di un cloud privato, può utilizzare le risorse di un cloud pubblico per gestire improvvisi picchi di lavoro che non possono essere soddisfatti facendo ricorso unicamente alle risorse disponibili nel cloud privato. Questa soluzione è facilmente implementabile quando il cloud privato è installato nello stesso data center del fornitore di servizi cloud Pubblici.

Un altro scenario possibile, invece, è quello in cui l'utente utilizza il suo cloud privato per portare a termine determinati task, ed utilizza uno o più cloud Pubblici per eseguirne altri. In questo scenario si pone il problema per l'utente di scegliere quali task eseguire nel cloud privato e quali nel cloud pubblico. Ad esempio, l'utente eseguirà nel cloud privato i task che coinvolgono dati che sono confidenziali, e nel cloud pubblico gli altri task.

Dal punto di vista dell'efficienza, invece, una caratteristica che potrebbe essere presa in considerazione dall'utente per scegliere su quali cloud eseguire le proprie applicazioni è il rapporto tra quantità di dati e tempo di computazione. Infatti, trasferire una grande quantità di dati su un cloud pubblico risulta conveniente solo quando deve essere eseguito un task che richiede un elevato tempo di computazione.

1.3 Modello concettuale e ruoli

Nella figura successiva viene riportata il modello concettuale di riferimento del cloud computing proposta dal NIST (*National Institute of Standards and Technology*) in cui sono riportati i principali attori, le attività e le funzioni da essi svolte nel cloud computing [NISTCCRA11].



Modello concettuale di riferimento

Nell'ambito di questo modello è possibile individuare cinque ruoli principali.

Cloud provider

Il cloud provider (o cloud service provider, CSP) è il soggetto responsabile di rendere il servizio utilizzabile alle parti terze interessate. Il cloud provider acquisisce e gestisce le infrastrutture elaborative necessarie a fornire i servizi, assicura l'esecuzione dei programmi che consentono i servizi, e le infrastrutture per erogare i servizi attraverso la rete.

Le attività del CSP coprono cinque aree principali che riguardano l'erogazione del servizio, l'orchestrazione del servizio, la gestione dei servizi cloud, la sicurezza e la privacy.

Cloud consumer

Il cloud consumer (o cloud service consumer, CSC) è il principale soggetto che utilizza i servizi di cloud computing. Un cloud consumer rappresenta una persona o una organizzazione che ha sottoscritto un contratto con un cloud provider. Il cloud consumer esamina il catalogo dei servizi di un cloud provider, richiede specifici servizi e li utilizza. Il cloud consumer utilizza degli accordi sui livelli di servizio (Service Level Agreements / SLAs) per specificare i requisiti sulle prestazioni tecniche che devono essere soddisfatti da un cloud provider. Un cloud provider potrebbe anche elencare negli SLA un insieme di restrizioni e obblighi che il cloud consumer deve accettare.

Cloud auditor

Il cloud auditor è il soggetto che può eseguire un esame indipendente sui controlli effettuati sui servizi con il fine di esprimere un parere nel merito. Il cloud auditor può valutare i servizi erogati da un cloud provider come ad esempio i controlli per la sicurezza, l'impatto sulla privacy e sulle prestazioni.

CLOUD BROKER

L'integrazione dei servizi cloud può risultare un'attività complessa da condurre per il cloud consumer, specie in un ambiente in forte evoluzione come è il cloud computing. Invece di contattare direttamente il cloud provider, il cloud consumer può pertanto richiedere i servizi cloud attraverso un cloud broker.

Il cloud broker è il soggetto che gestisce l'impiego, le prestazioni e l'erogazione dei servizi cloud e cura le relazioni tra il cloud provider ed il cloud consumer. In generale un cloud broker opera in tre aree:

- **intermediazione**: estende un servizio cloud fornendo servizi a valore aggiunto ai cloud consumer, per esempio la gestione dell'accesso, dell'identità o della sicurezza.
- **aggregazione**: combina e integra servizi diversi in un servizio nuovo, assicurando l'integrazione e la sicurezza dei dati trasferiti tra il cloud consumer e i differenti cloud provider.
- **arbitraggio**: sceglie i servizi cloud da fornitori diverse in modo flessibile e dinamico facendo ricorso a criteri di economicità o di disponibilità.

CLOUD CARRIER

Il cloud carrier agisce come un intermediario che fornisce la connettività ed il trasporto di servizi cloud tra il cloud consumer e il cloud provider. Il cloud carrier fornisce l'accesso al cloud consumer attraverso le reti e i dispositivi di accesso. Per esempio, i cloud consumer possono ottenere servizi cloud attraverso i dispositivi di accesso alla rete, come computer desktop, computer portatili, telefoni cellulari e altri dispositivi Internet mobili. La distribuzione dei servizi cloud è normalmente fornita dagli operatori di rete e di telecomunicazione.

2. OPPORTUNITÀ E RISCHI

Piuttosto che "cloud computing", l'espressione "servizi cloud" esprime meglio la principale innovazione costituta dalla progressiva trasformazione dell'ICT in un "bene standard" (*commodity*), acquistabile dai *Cloud Service Provider* (CSP) presenti sul mercato in forme essenzialmente equivalenti fra loro. Il cloud nelle sue diverse sfaccettature (IaaS/Paas/SaaS, privato/pubblico/di comunità/ibrido ecc.) interessa non solo per il risparmio e la razionalizzazione che può portare nei data centre ma per la prospettiva di realizzare infrastrutture condivise che facilitino drasticamente la progettazione, la realizzazione e la gestione dei sistemi informativi e, in definitiva, migliorino il rapporto tra Stato e cittadini. Come è già stato detto altrove [WEF10], con ogni evidenza il cambiamento innescato dal cloud si manifesterà per il 20% nella tecnologia e per l'80% nella società.

Pur in un quadro in rapida evoluzione, i servizi cloud si presentano come uno dei mezzi più economici per assicurare ad una gran parte dei servizi di eGovernment quelle caratteristiche di efficacia, efficienza, trasparenza, partecipazione, condivisione, cooperazione, interoperabilità e sicurezza previste dal Codice dell'Amministrazione Digitale [CAD05]. Tali obiettivi, peraltro, richiamano quelli concordati nella Dichiarazione Ministeriale di Malmö [MAL09], nel Piano d'azione europeo di eGovernment 2011 – 2015 [EUAP10] e nell'Agenda Digitale Europea [DAE10]. Le strategie di eGovernment di molti Paesi (tra i quali USA, UK, Francia, Giappone e Canada) puntano già con decisione alla promozione e all'adozione del cloud da parte dell'amministrazione statale. È attesa per la primavera 2012 la pubblicazione di una strategia cloud europea, annunciata dalla VP della Commissione UE Neelie Kroes [KRO11], la cui preparazione è stata accompagnata da numerosi studi e approfondimenti tecnici e da una vasta consultazione. La Commissione europea sta infine avviando la *European Cloud Partnership* [KRO12] che punta a concordare requisiti e standard adeguati al settore pubblico per promuovere il *procurement* di servizi cloud a livello europeo.

Per riassumere quanto detto nel precedente capitolo, le principali opportunità sembrano provenire da quattro caratteristiche del cloud computing.

- L'**elasticità** è un fattore rivoluzionario perché permetterà agli utenti e alle organizzazioni di svolgere rapidamente attività complesse precedentemente impedite da vincoli di costo o tempo. La possibilità di adattare l'intensità delle risorse quasi immediatamente consente un nuovo livello di sperimentazione ed evita i problemi derivanti dalla scarsità di risorse.
- L'**eliminazione delle spese di capitale** ridurrà significativamente il fattore di rischio dei progetti permettendo una maggiore sperimentazione. I costi di avvio di un'operazione risulteranno ridotti, come anche i costi di errori o di chiusura. Nel caso in cui un'applicazione non necessiti più di determinate risorse, queste possono essere sospese senza spese aggiuntive o procedure di annullamento.
- Il **provisioning self-service** dei server attraverso un semplice portale web anziché tramite un processo IT e una catena di approvazione complessi può ridurre le dispersioni nel modello di consumo, permettendo il provisioning e l'integrazione rapidi di nuovi servizi. Un sistema di questo tipo consente anche il completamento dei progetti in meno tempo, con meno rischi e un sovraccarico amministrativo minore rispetto al passato.
- La **riduzione della complessità** contrasta quello che è stato per molto tempo un fattore frenante dell'innovazione IT. Dal punto di vista dell'utente finale, le soluzioni SaaS (Software as a Service) stanno introducendo un nuovo ambiente software adatto all'utente. Dal punto di vista dello sviluppatore, le soluzioni PaaS (Platform as a Service) semplificano enormemente il processo di scrittura di nuove applicazioni.

Sia come acquirente che come fornitore di servizi cloud, la pubblica amministrazione si trova di fronte a complesse problematiche economiche, finanziarie, tecnologiche, giuridiche, contrattuali, organizzative e amministrative. In questo capitolo vengono descritti opportunità e rischi connessi ad alcuni di questi ambiti.

2.1 Aspetti tecnico-economici

L'economia ha un ruolo importante nel plasmare le trasformazioni di settore. Le attuali discussioni sul cloud si basano principalmente sulla complessità tecnica e sui problemi relativi all'adozione di questo ambiente. Sebbene l'esistenza e l'importanza di tali preoccupazioni siano innegabili, in genere gli aspetti economici di base hanno un impatto molto più forte sulla direzione e sulla velocità del cambiamento, in quanto le sfide tecnologiche vengono risolte o superate attraverso il rapido processo di innovazione a cui ci siamo abituati.

Nell'epoca del mainframe, l'ambiente client/server fu considerato inizialmente una sorta di tecnologia giocattolo, non adatta a sostituire l'ambiente mainframe. Tuttavia, con il passare del tempo, la tecnologia client/server si è diffusa sempre di più nelle aziende. In modo analogo, quando è stata proposta per la prima volta la tecnologia di virtualizzazione, la sua adozione è stata ostacolata da perplessità riguardo alla compatibilità tra le applicazioni. Tuttavia, le previsioni economiche di un risparmio del 20%-30% hanno presto convinto i responsabili dei sistemi informativi ad adottare rapidamente la tecnologia client-server.

Parallelamente si sono mosse le tecnologie relative alle piattaforme applicative nella direzione della modularità e della standardizzazione delle interfacce tra moduli in particolare con l'approccio SOA (*Service-Oriented Architecture*).

L'arrivo dei servizi cloud cambia ancora una volta l'economia del settore informatico. La tecnologia cloud standardizza e raggruppa le risorse IT e automatizza molte delle attività di manutenzione attualmente eseguite manualmente. Le architetture cloud favoriscono scenari di utilizzo flessibile, self-service e forme di pagamento a consumo. L'ambiente cloud può produrre risparmi e altri benefici economici in almeno quattro aree:

- impatto a livello macro-economico
- risparmi da parte dei cloud provider
- aggregazione della domanda
- efficienza del multi-tenancy

Impatto del cloud a livello macroeconomico

La diffusione del modello cloud può avere importanti conseguenze a livello macroeconomico, cioè sull'economia nel suo complesso, come peraltro è accaduto per le infrastrutture delle telecomunicazioni, il cui impatto è stato descritto attraverso specifici modelli econometrici.

Attraverso il cloud computing, le pubbliche amministrazioni e le imprese sono in grado di noleggiare capacità computazionale (sia hardware che software con elevati livelli di servizio) e capacità di storage da un service provider e pagare su domanda, come già in uso per altri servizi (per esempio la distribuzione dell'energia elettrica).

Questo ha un profondo impatto sulla struttura dei costi per tutti i soggetti che impiegano hardware e software, e quindi porta a cruciali conseguenze su:

- nascita di imprese ed aumento del prodotto nazionale sulle performance macroeconomiche;
- creazione di lavoro in tutte le industrie e riallocazione del lavoro nel settore ICT
- impatto sui conti della finanza pubblica, attraverso l'impatto diretto sulla spesa del settore pubblico e su quello indiretto delle entrate fiscali.

Una descrizione quantitativa di questi tre aspetti con riferimento all'economia dei paesi europei è stata fornita in [ETR09] attraverso uno specifico modello econometrico. Il primo risultato del modello è che il cloud computing può creare alcune centinaia di migliaia di nuove piccole imprese in Europa, e in particolare nel nostro Paese, con un impatto significativo sull'occupazione e sulla riduzione del tasso di disoccupazione di qualche punto decimale. L'impatto netto risultante sull'occupazione deriva dal rapporto stimato di 8:1 tra nuovi lavori che si creano in tutti i settori e lavori di tipo tradizionale persi nel settore ICT. Questo comporta che il problema della riallocazione del lavoro all'interno dei

dipartimenti o nei dipartimenti IT dei settori collegati risulta limitato. Il secondo risultato del modello è l'impatto sulla crescita del PIL è compreso fra lo 0,05% e lo 0,3%.

Perciò, l'introduzione del cloud computing che già di per sé porta ad una riduzione dei costi, può avere un non trascurabile ulteriore impatto positivo sulla finanza pubblica che va al di là della semplice riduzione del costo del settore pubblico. Questo accade perché la finanza pubblica beneficia da un lato dalla riduzione dei costi, e dall'altro lato dalle entrate fiscali derivanti dalla crescita delle attività economiche e dalla creazione di nuove imprese private e dei relativi posti di lavoro.

ECONOMIE DI SCALA PER I CLOUD PROVIDER

Il cloud computing combina le migliori proprietà economiche degli ambienti mainframe e client-server.

L'era del mainframe è stata caratterizzata da economie di scala significative accompagnate da elevati costi iniziali dei mainframe e dalla necessità di assumere personale specializzato per la gestione dei sistemi. Con l'aumentare della richiesta di capacità di elaborazione, all'inizio i costi sono scesi rapidamente, ma solo le organizzazioni IT centralizzate di grandi dimensioni hanno potuto contare sulle risorse e sulla domanda aggregata indispensabili per giustificare un investimento di questo tipo.

Con l'avvento dei minicomputer e, più tardi, della tecnologia client-server, l'unità di acquisto minima è stata ridotta significativamente e le risorse sono diventate più semplici da utilizzare e gestire. Questa modularizzazione ha sensibilmente abbassato le barriere di accesso alla fornitura dei servizi IT, migliorando radicalmente l'agilità dell'utente finale. Ciò ebbe però un effetto negativo sull'utilizzo, che diede come risultato la situazione attuale, ovvero data center pieni di server acquistati per varie esigenze, ma funzionanti solo al 5%-10% delle loro possibilità.

Il cloud computing garantisce agli utenti economie di scala e un'efficienza superiori a quelle dei mainframe nella loro configurazione tradizionale, abbinate a una modularità e un'agilità migliori di quelle offerte dalla tecnologia client-server, eliminandone gli effetti negativi.

Le economie di scala derivano da quattro aree.

- **Costo dell'energia**. Il costo dell'energia elettrica sta aumentando rapidamente e sta diventando l'elemento più importante del costo totale di proprietà (TCO) rappresentandone attualmente il 15%-20%. L'efficienza nell'uso dell'energia tende a essere decisamente inferiore nelle strutture più grandi rispetto a quelle di dimensioni ridotte. Mentre gli operatori dei piccoli data center devono pagare le normali tariffe locali per l'elettricità, i provider di grandi dimensioni possono pagare meno di un quarto della tariffa media nazionale grazie alla possibilità di collocare i propri data center in luoghi in cui l'energia elettrica costa meno e ottenendo vantaggiosi contratti a volume.
- **Costi del lavoro per l'infrastruttura**. Il cloud computing consente di ridurre decisamente i costi del lavoro a qualsiasi livello automatizzando molte attività di gestione ripetitive, ma le strutture più grandi possono registrare riduzioni maggiori rispetto a quelle di dimensioni ridotte. Un solo amministratore di sistema può seguire pochi server in una pubblica amministrazione tradizionale, mentre in un cloud data center lo stesso amministratore è in grado di seguirne migliaia.
- **Sicurezza e affidabilità**. Sebbene sia spesso considerata come un possibile problema per l'adozione dell'ambiente cloud, la crescente esigenza di sicurezza e affidabilità favorisce le economie di scala a causa del livello di investimento prevalentemente fisso necessario per ottenere sicurezza e affidabilità operative. I grandi provider commerciali di servizi cloud sono spesso più adatti a garantire la competenza necessaria a risolvere questo problema rispetto al tipico reparto IT di un'azienda e ciò rende i sistemi cloud più sicuri e affidabili.
- **Potere di acquisto**. Gli operatori di data center di grandi dimensioni possono ottenere sconti elevati sull'hardware acquistato rispetto agli acquirenti normali.

I fornitori di servizi cloud hanno iniziato a creare data center di dimensioni senza precedenti, ed è probabile che con il tempo si potranno ottenere economie di scala ancora difficili da stimare. Per questo motivo, i maggiori fornitori di servizi cloud otterranno maggiori vantaggi, in linea generale, rispetto alle aziende o alle pubbliche amministrazione che utilizzano data center interni di minori dimensioni.

ECONOMIE DI SCALA LEGATE ALLA DOMANDA

Il costo globale dell'IT è determinato non solo dal costo della capacità, ma anche dal grado di efficienza nell'utilizzo di tale capacità. È quindi necessario valutare l'impatto che l'aggregazione della domanda avrà sui costi delle risorse effettivamente utilizzate (CPU, rete e archiviazione).

In un data center non virtualizzato, ogni applicazione o carico di lavoro viene in genere eseguito in un server fisico dedicato. Ciò significa che il numero dei server è direttamente proporzionale al numero dei carichi di lavoro. In questo modello, l'utilizzo dei server è sempre stato estremamente basso, intorno al 5% - 10%. La virtualizzazione consente l'esecuzione di più applicazioni in un unico server fisico all'interno della relativa istanza del sistema operativo, pertanto il vantaggio principale della virtualizzazione sta nel fatto che è necessario un numero minore di server per gestire lo stesso numero di carichi di lavoro .

Ma quali effetti ha questa situazione sulle economie di scala? Se tutti i carichi di lavoro avessero un'attività costante, ciò implicherebbe una semplice compressione delle unità senza influenzare le economie di scala. In realtà, tuttavia, i carichi di lavoro variano significativamente con il tempo e spesso richiedono grandi quantità di risorse in una determinata situazione e quasi nessuna a distanza di poco tempo. Si aprono quindi opportunità per miglioramenti in termini di utilizzo tramite l'aggregazione e la diversificazione della domanda.

Analizzando le diverse fonti di variabilità del livello di utilizzo e considerando le possibilità di diversificazione dell'ambiente cloud per una conseguente riduzione dei costi è possibile individuare cinque fonti di variabilità e valutare come possono essere ridotte.

- **Casualità**. I modelli di accesso degli utenti finali contengono un certo grado di casualità. Per esempio, gli utenti controllano la posta elettronica in momenti diversi. Per rispettare i contratti di servizio, i buffer di capacità devono essere progettati tenendo conto di una certa probabilità che molte persone eseguano attività specifiche contemporaneamente. Se i server sono raggruppati in pool, la variabilità può essere ridotta.
- **Modelli orari**. Nel comportamento degli utenti sono presenti cicli ricorrenti quotidiani: i servizi per i consumatori tendono a raggiungere i picchi alla sera, mentre i servizi per i luoghi di lavoro registrano picchi durante la giornata lavorativa. La capacità deve essere progettata tenendo conto di tali picchi giornalieri e dei momenti in cui il servizio registrerà uno scarso utilizzo. Questa variabilità può essere bilanciata eseguendo lo stesso carico di lavoro per più fusi orari sugli stessi server oppure eseguendo carichi di lavoro con modelli orari complementari (per esempio i servizi per i consumatori e i servizi per le aziende) sugli stessi server.
- **Variabilità specifiche del settore**. Alcune variabilità dipendono dalle dinamiche di settore. Tipicamente, i rivenditori registrano picchi durante i periodi di maggiori acquisti, mentre le società contabili USA registrano un picco prima del 15 aprile, scadenza di presentazione della dichiarazione dei redditi. Esistono diversi tipi di variabilità di settore: alcune sono ricorrenti e prevedibili (per esempio il periodo della dichiarazione dei redditi o i Giochi Olimpici), mentre altre sono imprevedibili (per esempio le notizie del giorno). Il risultato comune è che è necessario garantire la capacità per il periodo di picco previsto, più un margine di errore. Gran parte di questa capacità non servirà per il resto del tempo. La diversificazione offre importanti vantaggi per ridurre le variabilità di settore.
- **Variabilità di utilizzo delle risorse**. Le risorse di elaborazione, archiviazione e di input/output (I/O) vengono in genere acquistate insieme: un server contiene una certa quantità di potenza di elaborazione (CPU), archiviazione e I/O (per esempio i servizi di rete o l'accesso al disco). Alcuni carichi di lavoro come quelli delle ricerche utilizzano molta CPU ma relativamente poco spazio di archiviazione o I/O, mentre altri come la posta elettronica tendono a utilizzare molto spazio di archiviazione ma poca CPU. Sebbene sia possibile controllare la

capacità acquistando server ottimizzati per fornire CPU o spazio di archiviazione, in questo modo si risolve solo in parte il problema, in quanto la flessibilità risulta ridotta e la soluzione potrebbe non essere economica dal punto di vista della capacità. Questa variabilità comporterà la presenza di risorse inutilizzate, a meno che non si applichi la diversificazione dei carichi di lavoro eseguendo carichi di lavoro con profili di risorse complementari.

- **Modelli di crescita incerti**. La difficoltà nel prevedere quali risorse informatiche saranno necessarie in futuro e l'elevato tempo di risposta necessario per portare la capacità online sono altri motivi di scarso utilizzo. Tutte le pubbliche amministrazioni devono ottenere l'approvazione per gli investimenti IT con largo anticipo rispetto alla conoscenza diretta della richiesta di infrastrutture. Le amministrazioni più grandi devono affrontare questo problema pianificando i propri acquisti con circa dodici mesi di anticipo. Diversificando l'attività con carichi di lavoro di vari clienti, i provider di servizi cloud possono ridurre queste incertezze, in quanto la richiesta superiore alle aspettative di alcuni carichi di lavoro verrà annullata da una domanda inferiore al previsto per altri.

Un vantaggio economico importante del cloud è la possibilità di risolvere i problemi legati alla variabilità nell'utilizzo delle risorse che dipende da tali fattori. Raggruppando le risorse, la variabilità viene diversificata e vengono creati modelli di utilizzo uniformi. Più ampio è il pool di risorse, più semplice sarà il profilo della domanda aggregata, maggiore sarà la percentuale generale di utilizzo e più economico ed efficiente sarà per l'organizzazione IT soddisfare le richieste degli utenti finali. Abbiamo modellato l'impatto teorico della variabilità casuale della domanda sulle percentuali di utilizzo dei server man mano che aumenta il numero dei server

Un pool teorico di 1.000 server può essere eseguito a circa il 90% di utilizzo senza violare il contratto di servizio. Ciò vale solo nella situazione ipotetica in cui la variabilità casuale è l'unica fonte di variabilità e i carichi di lavoro possono essere sottoposti a migrazione tra server fisici immediatamente senza interruzioni. Si noti che i livelli superiori di tempo di attività (definiti nel contratto di servizio o SLA) diventano molto più semplici da garantire con l'aumentare della scala.

Gli ambienti cloud saranno in grado di ridurre la variabilità oraria, a condizione che vengano diversificati con luoghi geografici e tipi di carico di lavoro diversi.

In un'organizzazione media, l'uso delle risorse IT in una situazione di picco può arrivare al doppio della media giornaliera. Anche in organizzazioni di grandi dimensioni distribuite in aree geografiche diverse la maggior parte dei dipendenti e degli utenti vive in aree simili e pertanto i loro cicli quotidiani saranno quasi sincroni. Inoltre, molte organizzazioni non hanno solitamente modelli di carico di lavoro opposti: per esempio le attività di elaborazione della posta elettronica, del traffico di rete e delle transazioni che vengono eseguite durante gli orari di ufficio non corrispondono a un flusso di lavoro ugualmente attivo durante la notte. Raggruppando organizzazioni e carichi di lavoro di tipo diverso è possibile compensare gli alti e i bassi dell'attività.

La variabilità di settore provoca picchi altamente correlati e momenti di inattività in ogni azienda. Ciò significa che la maggior parte dei sistemi di un rivenditore raggiungerà la capacità massima durante i periodi di vacanza (per esempio i server Web, i sistemi di elaborazione delle transazioni e di gestione dei pagamenti, i database).

Parte della variabilità legata a modelli di crescita incerti può essere ridotta con la standardizzazione dell'hardware e la fornitura just-in-time, anche se non del tutto. L'impatto dell'incertezza nella crescita per le Amministrazioni con un massimo di poche decine di server è molto superiore rispetto a quello di un servizio pubblico cloud. Per le Amministrazioni più piccole (per esempio i piccoli comuni), l'impatto è ancora maggiore.

Si noti che anche i cloud pubblici più grandi non saranno in grado di diversificare tutte le variabilità. Probabilmente rimarrà la variabilità a livello di mercato. Per semplificare ulteriormente la domanda, è possibile impiegare un sistema di definizione dei prezzi complesso. Per esempio, in modo analogo al mercato dell'energia elettrica, i clienti possono essere incentivati a spostare la domanda da periodi di utilizzo intenso a periodi di utilizzo ridotto. Inoltre, prezzi più

bassi incoraggiano un aumento dell'utilizzo da parte dei clienti grazie all'elasticità dei prezzi. La gestione della domanda aumenterà ulteriormente i vantaggi economici dell'ambiente cloud.

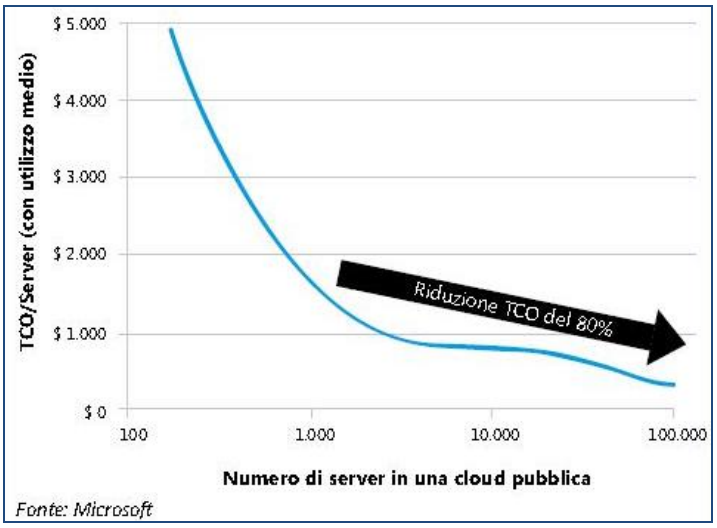
ECONOMIE DI SCALA DEL MULTI-TENANCY

Le economie di scala relative ai fornitori e alla domanda descritte in precedenza possono essere ottenute indipendentemente dall'architettura delle applicazioni, sia essa un adattamento tradizionale, una soluzione per un singolo cliente o per più clienti. Esiste un'altra importante fonte di economie di scala che può essere sfruttata solo se le applicazioni sono scritte come applicazioni multi-tenant. Infatti, anziché eseguire un'istanza di un'applicazione per ogni cliente, come accade per le applicazioni locali e per la maggior parte delle applicazioni ospitate, in un'applicazione multi-tenant più clienti utilizzano simultaneamente un'unica istanza dell'applicazione. Ne derivano due importanti vantaggi economici:

- I costi fissi di manutenzione delle applicazioni sono ammortizzati su un numero elevato di clienti. In un'istanza single-tenant, ogni cliente deve pagare la gestione della propria applicazione, ovvero il lavoro associato alla gestione degli aggiornamenti e alla risoluzione dei problemi. Nelle istanze dedicate, le stesse attività, come l'applicazione di patch software, vengono eseguite più volte: una volta per ogni istanza. In un'istanza multi-tenant, tale costo viene condiviso da un numero elevato di clienti, pertanto il costo di manutenzione delle applicazioni per ogni cliente è prossimo a zero. Questo può portare a una riduzione significativa del costo complessivo, in particolare per applicazioni complesse.
- L'utilizzo fisso di componenti server è ammortizzato su un numero elevato di clienti. Per ogni istanza di un'applicazione esiste una certa quantità di utilizzo del server. Passando a un modello multi-tenant con una sola istanza, questo sovraccarico delle risorse può essere ammortizzato tra più clienti. Le applicazioni possono essere completamente multi-tenant se vengono scritte per avvalersi di tali vantaggi oppure possono offrire funzionalità di multi-tenancy parziale utilizzando i servizi condivisi forniti dalla piattaforma cloud. Maggiore è l'utilizzo di tali servizi condivisi, maggiore saranno i vantaggi che l'applicazione otterrà da tali economie di scala del multi-tenancy.

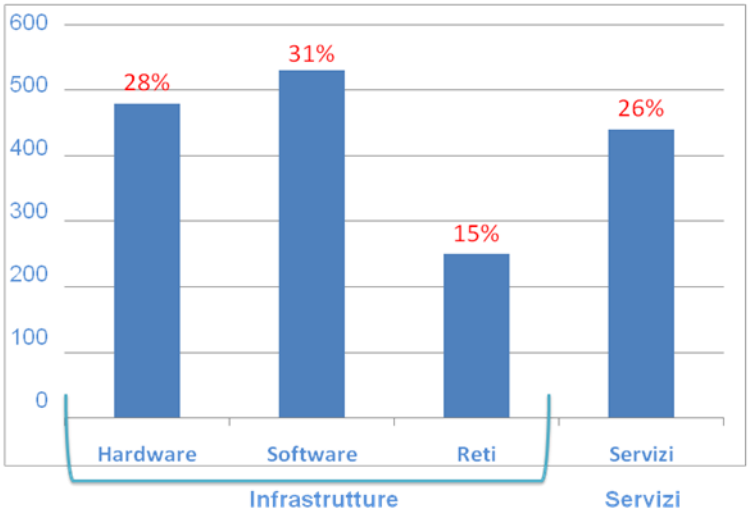
ECONOMIE DI SCALA DEI CLOUD PUBBLICI

La combinazione di economie di scala per i cloud provider relative alla capacità dei server (ammortizzazione dei costi su più server), l'aggregazione dei carichi di lavoro per i clienti (riduzione della variabilità) e il modello di applicazioni multi-tenant (ammortamento dei costi su più clienti) genera potenti economie di scala. Per stimarne la portata, sono stati creati modelli che stimano il comportamento a lungo termine dei costi. Dalla figura successiva si deduce che un data center con 100.000 server ha un costo totale di proprietà (o TCO, *Total Cost of Ownership*) inferiore del 90% rispetto a un data center con 500 server e dell'80% rispetto a un data center con 1.000 server.



Economie di scala dell'ambiente cloud

Questa situazione ci porta a valutare l'impatto degli aspetti economici dell'ambiente cloud sul budget IT. Dai dati della PA centrale, possiamo valutare l'abbattimento approssimativo tra i costi di infrastrutture (hardware, software, reti) ed i costi dei servizi (che comprendono i costi di supporto e gestione delle applicazioni esistenti e i costi di sviluppo di nuove applicazioni). L'ambiente cloud ha un effetto su tutte e due le aree. I risparmi per la fornitura e per la gestione della domanda riguardano principalmente la parte dell'infrastruttura, che allo stato attuale comprende oltre il 70% della spesa complessiva, mentre la parte servizi (che comprende lo sviluppo di nuove applicazioni) riguarda meno del 30% della spesa.



fonte: Cnipa – Relazione annuale sullo stato dell'ICT nella PAC 2008

Scomposizione della spesa informatica della PAC

Gli aspetti economici descritti avranno un impatto profondo sull'IT. Molti responsabili dei sistemi informativi delle pubbliche amministrazioni devono attualmente scontrarsi con il fatto che il 70% del budget viene speso per mantenere le infrastrutture esistenti. Rimangono quindi poche risorse non solo per introdurre l'innovazione nei data center ma anche soltanto per adeguarne la capacità. Il cloud computing libererà importanti risorse, sia nell'area delle infrastrutture che in quella dei servizi, che possono essere destinate all'innovazione.

Economie dei cloud privati

I cloud pubblici si differenziano da quelli privati in base al fatto che le risorse IT sono condivise tra molte organizzazioni distinte (cloud pubblico) o dedicate a una sola organizzazione (cloud privato). Se confrontate con i data center virtualizzati tradizionali, i cloud pubblici e privati si avvalgono della gestione automatizzata (per risparmiare su attività ripetitive) e hardware omogeneo (per ridurre il costo e aumentare la flessibilità). A causa della natura ampiamente condivisa dei cloud pubblici, una differenza principale tra cloud pubblici e privati sta nella scala e nel livello a cui riescono a raggruppare la domanda.

- I data center virtualizzati tradizionali consentono in genere il raggruppamento delle risorse all'interno di confini di organizzazioni esistenti, ovvero il gruppo IT dell'azienda virtualizza i propri carichi di lavoro, mentre i reparti possono decidere se fare lo stesso. In questo modo è possibile diversificare alcune delle variabilità casuali, orarie (in particolare se l'azienda ha uffici in tutto il mondo) e specifiche del carico di lavoro, tuttavia le dimensioni del pool e la difficoltà di spostare carichi da una macchina virtuale a un'altra (peggiorata dalla mancanza di omogeneità delle configurazioni hardware) limita la possibilità di ottenere tutti i vantaggi descritti. Questo è uno dei motivi per cui anche i data center virtualizzati non vengono ancora utilizzati

appieno. Non ci sono modifiche del modello di applicazione, pertanto la complessità della creazione di applicazioni non viene ridotta.

- I cloud privati vanno oltre la virtualizzazione. Le risorse sono raggruppate in pool all'interno dell'azienda, anziché in base all'unità organizzativa, e i carichi di lavoro vengono spostati senza problemi tra server fisici per garantire l'efficienza e la disponibilità ottimali. Ciò riduce ulteriormente l'impatto della variabilità casuale, oraria e del carico di lavoro. Inoltre, i nuovi modelli di applicazione ottimizzati per il cloud (PaaS) permettono lo sviluppo più efficiente di applicazioni e garantiscono costi operativi più bassi.
- I cloud pubblici hanno gli stessi elementi dell'architettura dei cloud privati, tuttavia offrono una scala decisamente maggiore per supportare tutte le fonti di variabilità. I cloud pubblici sono anche l'unica soluzione per diversificare le variabilità specifiche del settore, l'elemento completamente geografico della variabilità oraria e fornire i vantaggi del multi-tenancy.

I cloud privati possono risolvere alcuni dei problemi di adozione dei cloud pubblici. Disponendo di hardware dedicato, sono più facili da utilizzare all'interno del firewall aziendale, il che può risolvere i problemi di sicurezza e privacy. Se si rende locale un cloud privato, può risultare più semplice risolvere alcuni problemi di normative, conformità e sovranità che possono presentarsi nel caso di servizi che oltrepassano confini giuridici. Nei casi in cui questi fattori abbiano grande importanza per una decisione da parte dei responsabili dei sistemi informativi, un investimento in un cloud privato può essere la soluzione migliore.

I cloud privati non sono in realtà diverse dai cloud pubblici per quanto riguarda gli altri problemi, quali la maturità e le prestazioni. Le tecnologie dei cloud pubblici e privati si stanno sviluppando insieme e matureranno insieme.

2.2 Aspetti giuridici

I numerosi profili giuridici sollevati dal cloud computing sono oggetto di un dibattito avviato solo di recente e ben lungi dal concludersi. La materia è ancora magmatica e sono rare al momento le analisi approfondite e di dettaglio, e ancor meno sono disponibili approfondimenti sui risvolti contrattuali. Per questo è corretto avvertire che le linee tracciate sono necessariamente soggette a mobilità e che l'inquadramento di carattere generale tentato in questo lavoro va correttamente inteso come un contributo alla discussione piuttosto che come un approdo definitivo.

Occorre evidenziare che non esistono attualmente delle disposizioni specifiche, nazionali o comunitarie, che disciplinino i contratti di cloud computing e che gli strumenti contrattuali attualmente proposti dai cloud provider appartengono prevalentemente alla categoria dei contratti c.d. "per adesione" nei quali, sostanzialmente, le clausole non sono negoziabili e sovente non definiscono aspetti assai delicati (ad es. responsabilità, livelli di servizio, legge applicabile,ecc.) rischiando, quindi, di non garantire la necessaria coerenza alle disposizioni che disciplinano in Italia gli appalti pubblici.

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.

Appalto di servizi o contratto atipico

La qualificazione giuridica di un contratto di servizi cloud risulta essenziale al fine di determinare quale sarà la disciplina giuridica che si renderà applicabile ai rapporti tra le parti contrattuali (PA e fornitore) e, di conseguenza, quali clausole è opportuno che siano presenti nel contratto.

Si possono al riguardo riportare alcune valutazioni espresse in [BEL11]:

> "Da un lato, con particolare riferimento ai sistemi di cloud computing di tipologia SaaS ed alla loro riconducibilità al fenomeno dell'outsourcing, una parte degli interpreti, ritiene che il contratto che si stipula per l'utilizzo di un sistema di SaaS possa inquadrarsi nello schema dell'appalto di servizi. Dall'altro lato, altri

autori, non condividendo la tesi sopra enunciata, sostengono che quello di fornitura di servizi di cloud computing rappresenti una particolare figura di contratto atipico."

[BEN08] precisa che l'inquadramento del contratto di cloud tra quelli di appalto di servizi comporta che:

> "la prevalenza di una prestazione di fare, avente ad oggetto la fornitura di uno o più servizi software o di altra natura, unitamente alla presenza di una organizzazione dotata di mezzi e gestione propri ed al pagamento di un corrispettivo sono tutti elementi che fanno propendere per la configurabilità di un appalto di servizi, sia pure avente ad oggetto prestazioni continuative o periodiche. La prima diretta conseguenza di tale inquadramento è che l'obbligazione dell'appaltatore costituisce una obbligazione di risultato, anche se nella pratica non mancano casi di soggetti interessati a far figurare nel contratto i propri obblighi come di mezzi."

Alle stesse conclusioni perviene, dopo ampie argomentazioni, anche [BEL11] concludendo che si può ritenere in via generale - salvo casi particolari - che il contratto di fornitura di servizi di cloud rientri nella categoria dell'appalto di servizi disciplinato dagli articoli 1655 e ss. del codice civile.

La dottrina che invece sostiene che il contratto di cloud vada collocato tra i "contratti atipici" parte dalla considerazione in base alla quale (sempre con riferimento ai contratti di tipo SaaS) i servizi non vengono realizzati di volta in volta per i singoli utenti, ma questi ultimi si limitano ad utilizzare servizi già precedentemente realizzati. Tale circostanza non consentirebbe di far rientrare il contratto cloud tra quelli di appalto di servizi.

Tale dottrina ritiene, invece, che occorre considerare le peculiari caratteristiche del contratto che consente all'utente, tramite internet, di collegarsi ai server del cloud provider senza vincoli legati all'ubicazione fisica dell'utente medesimo, assicura una notevole flessibilità e scalabilità dei servizi che possono essere utilizzati sulla base dell'esigenza dell'utente, commisura il prezzo del servizio all'effettiva intensità di utilizzazione dello stesso. Tali peculiari caratteristiche porterebbero a qualificare il contrato cloud (di tipo SaaS) tra i c.d. contratti atipici.

Sulla base di quanto ad oggi valutabile riguardo la qualificazione giuridica del contratto di cloud computing, con particolare riferimento alla tipologia SaaS, e considerata l'attuale assenza di specifiche disposizioni normative e interpretazioni giurisprudenziali al riguardo, si ritiene che la qualificazione giuridica dei contratti in esame più convincente sia quella di un appalto di servizi disciplinato dalle disposizioni del codice civile applicabili anche in caso di appalti pubblici di servizi, come espressamente previsto dalle disposizioni del Codice degli appalti (D. Lgs. 163/2006).

IL CLOUD E LA NORMATIVA SUGLI APPALTI PUBBLICI

L'approfondimento delle problematiche e delle prospettive di sviluppo del cloud nel contesto delle pubbliche amministrazioni non può prescindere dal quadro normativo vigente in materia di contratti pubblici. Infatti, l'utilizzazione di un sistema basato su cloud computing prevede l'affidamento a terzi di una o più attività che hanno ad oggetto determinati servizi e prestazioni informatiche e di connettività erogati da soggetti privati (provider e gestore del sistema).

L'uso del cloud consente di svolgere operazioni piuttosto complesse o, comunque, particolarmente costose in termini di capacità di gestione delle richieste da parte di un soggetto terzo che esercita attività di impresa. Ne deriva che la natura dell'attività svolta dal medesimo provider/gestore presuppone l'esistenza di una vera e propria organizzazione di impresa senza la quale non sarebbe gestibile un sistema basato sul modello cloud. Si pensi, a mero titolo di esempio, alla struttura informatica necessaria a gestire servizi integrati di posta elettronica, produzione documentale e memorizzazione di dati e a come la stessa richieda risorse hardware e software particolarmente complesse. Chi eroga tale tipologia di servizi e forniture si assume il rischio del risultato da perseguire.

La complessità dei compiti di un fornitore di servizi cloud, che dovrà trovare espressione a livello contrattuale, dipende fortemente dal livello di delega esercitato per conto dei suoi clienti. I servizi erogabili in modalità cloud possono in linea di principio spaziare dagli **strumenti** tecnologici (come i tipici servizi IaaS e PaaS), ai **componenti** funzionali (ad esempio

elementi di sistemi IT complessi) fino alle **prestazioni** erogate ai clienti finali. Per meglio esplicitare questa differenza, una pubblica amministrazione potrebbe acquisire servizi cloud per finalità tanto diverse come l'esternalizzazione sul cloud di una parte del proprio data center sotto forma di macchine virtuali, del sistema di posta elettronica o di intere funzioni amministrative (come ad esempio la gestione delle dichiarazioni dei redditi).

A parte le problematiche connesse alla qualificazione giuridica del contratto che prevede erogazione di prestazioni in modalità cloud, è certo che la PA che voglia fare ricorso al cloud computing dovrà sottoscrivere un contratto con un operatore particolarmente qualificato e per far questo, non potendo determinarsi sul mercato come un qualsiasi privato, dovrà seguire il procedimento di aggiudicazione secondo le regole dell'evidenza pubblica.

La pubblica amministrazione che voglia acquisire prodotti e servizi cloud, pertanto, dovrà seguire le regole procedimentali necessarie per l'individuazione dell'operatore economico contraente e dovrà sottoscrivere con tale soggetto un contratto pubblico ai sensi del D. Lgs. n. 163/2006 e del relativo regolamento di esecuzione approvato con D.P.R. 207/2010.

La scelta da parte della PA di utilizzare la soluzione cloud per soddisfare le proprie esigenze, tenendo conto anche delle tipologie di cloud che si intende adottare, può trovare utili indicazioni in una **analisi comparativa** delle soluzioni, prevista dall'art. 68 del D. Lgs. 82/2005 – Codice dell'amministrazione digitale, e in uno **studio di fattibilità**. Si rileva infatti che l'art. 13 del D. Lgs. 39/1993 dispone che la stipulazione da parte delle amministrazioni di contratti per la progettazione, realizzazione, manutenzione, gestione e conduzione operativa di sistemi informativi automatizzati, determinati come contratti di grande rilievo ai sensi dell'art. 9 e dell'art. 17, è preceduta dall'esecuzione di studi di fattibilità volti alla definizione degli obiettivi organizzativi e funzionali dell'amministrazione interessata. Qualora lo studio di fattibilità sia affidato ad impresa specializzata, questa non ha facoltà di partecipare alle procedure per l'aggiudicazione dei contratti sopra menzionati (cfr. anche strategie di Acquisizione delle Forniture ICT - Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione - Manuale applicativo).

- La stazione appaltante utilizzando le indicazioni derivanti da tali attività potrà individuare la tipologia di cloud in grado di rispondere meglio alle proprie necessità, cercando di bilanciare, in funzione di tale scelta, l'esigenza di efficienza e di risparmio del denaro pubblico (in termini di economicità) da una parte, e quella della sicurezza della conservazione dei propri dati.

- In tale prospettiva, per la realizzazione di un cloud pubblico sarà necessario in primo luogo adottare una puntuale determina a contrarre (art. 11, comma 2, del D. Lgs. 163/2006) che con puntuale motivazione dia atto delle valutazioni che sono state eseguite per ritenere conveniente e opportuna l'introduzione di un sistema informativo basato sul cloud, tenuto conto che tale scelta implica una "rottura" determinante con il passato.

- La stazione appaltante sarà tenuta al rispetto delle linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione.

- Anche per i progetti relativi ad iniziative di cloud computing la pubblica amministrazione, se rientrante tra i soggetti destinatari delle disposizioni del D. Lgs. 39/1993 già richiamato, dovrà richiedere, prima di avviare la gara e qualora l'importo superi le relative soglie attualmente stabilite, il parere di congruità a DigitPA.

Altro aspetto di indubbio interesse è quello della determinazione dell'importo a base di gara. Tale importo dovrà essere determinato secondo le disposizioni previste dall'art. 29 del D. Lgs. 163/2006. In particolare, per i servizi cloud occorre considerare l'effettivo servizio ritenuto necessario e da mettere a gara sulla base delle esigenze che la pubblica amministrazione deve soddisfare. La determinazione dell'importo a base di gara potrà, quindi, determinarsi tramite una preliminare analisi dei costi, che consideri le varie componenti necessarie all'erogazione del servizio, quali, ad esempio, l'utilizzazione di un'infrastruttura hardware e software (considerando se dedicata o meno), da valorizzare sulla base di prezzi medi di mercato, il numero di risorse professionali da utilizzare, valorizzate sulla base delle tariffe

professionali unitarie medie di mercato, i livelli di servizio minimi richiesti, eventuali facoltà di recesso anticipato da parte della PA.

Certamente potrà essere individuato quale fornitore di servizi cloud uno dei soggetti rientranti nell'ambito dell'art. 34 del Codice (qualsiasi operatore economico singolo o riunito). La stazione appaltante dovrà definire con particolare attenzione i requisiti minimi economico-finanziari e tecnico-organizzativi di partecipazione che risultino i più aderenti alle proprie effettive esigenze, al fine di precludere la partecipazione a coloro che non sono in possesso della necessaria preparazione competenza e professionalità per poter eseguire un appalto verosimilmente complesso ma nel contempo non prevedendo dei requisiti minimi eccessivamente stringenti che determinerebbero una limitata partecipazione alla gara con conseguente violazione dei principi comunitari relativi alla concorrenza.

In altri paesi il fornitore di prodotti cloud viene sottoposto ad una forma di certificazione che lo qualifica come soggetto idoneo a trattare con la PA. In Italia in assenza di modalità di qualificazione specifica di un fornitore cloud si dovrà comunque richiedere un elevato standard qualitativo del sistema di qualificazione del concorrente (artt. 41 e 42 del Codice) previsto dalla normativa vigente. Il criterio da utilizzare per individuare l'aggiudicatario fornitore dovrebbe essere quello dell'offerta economicamente più vantaggiosa (art. 83 del Codice) che consente la valutazione tecnico qualitativa della soluzione proposta (pregio tecnico, proprietà, affidabilità, manutenzione), sulla base delle specifiche tecniche, anche consentendo agli operatori concorrenti di proporre in sede di offerta soluzioni progettuali innovative, senza limitare le offerte ad un solo modello specifico di soluzione informatica, con la possibilità di premiare la proposta più rispondente alle esigenze della PA.

2.3 *Privacy* e sicurezza

Con riferimento alla costante evoluzione del tracciato disegnato dal giurista, è da sottolineare la complessiva operazione di riforma, ormai imminente, della Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ("Direttiva 95/46/CE"). Si tratta di un intervento di portata sostanziale, che produrrà verosimilmente effetti strutturali di ampio raggio con ricadute prevedibili anche in tema di cloud.

Vanno comunque attese le posizioni ufficiali del Garante italiano per la protezione dei dati personali e, a livello europeo, del Gruppo di lavoro art. 29 per la protezione dei dati ("Gruppo ex art. 29"). Entrambe queste autorità hanno al momento affrontato solo alcuni aspetti della disciplina del cloud computing, riservando a futura occasione i necessari approfondimenti di sostanza.

Esaurita questa doverosa premessa e venendo al vivo dell'analisi, si pone innanzitutto la scelta dei modelli su cui soffermarsi. Si può infatti affrontare il tema del cloud secondo la prospettiva della pubblica amministrazione ("PA") nella veste di fornitrice (*provider*) di servizi cloud (per altre PA o per privati) oppure secondo quella della PA nel ruolo di fruitrice (*buyer*) di servizi cloud forniti da terzi (PA o privati). I due approcci sollevano questioni diverse e non necessariamente simmetriche. Soltanto a titolo di esempio, ci si deve preliminarmente chiedere, nell'ipotesi di PA *provider*, se non venga in considerazione (o fino a che punto non venga in considerazione) l'inquadramento della stessa nella tipologia del soggetto pubblico economico, con conseguente applicazione della disciplina prevista per i soggetti privati in tema di protezione dei dati personali.

Ad ogni modo, la presente analisi si sofferma unicamente sull'ipotesi della PA in veste di fruitrice di servizi cloud, possibilità che si prospetta al momento come di più immediata applicazione pratica.

Come già ricordato, le motivazioni per le quali un soggetto pubblico può valutare se migrare i propri dati in un cloud possono sinteticamente riassumersi in termini di risparmio economico, di interoperabilità e facilità di condivisione, di efficienza e di sicurezza.

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. 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.

Un'ulteriore obiezione di carattere generale che viene mossa in ambito privacy al cloud computing riguarda il mantenimento del controllo sui dati, principio fondamentale e di lontana formulazione. Aspetto complementare al controllo dell'interessato, e con esso necessariamente interrelato, è rappresentato dal controllo sui dati della PA come titolare del trattamento e, conseguentemente, del cloud provider sui dati distribuiti nel cloud. Il passaggio si lega a quello della ridondanza: occorre che le informazioni personali possano essere effettivamente e agevolmente modificate o cancellate, con effetto su tutte le copie presenti nel sistema. Ancora una volta viene in considerazione un elemento che si presta ad essere efficacemente affrontato innanzitutto a livello tecnico, essendo pacifico il principio giuridico a monte.

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 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.

Vi sono ulteriori obiezioni di natura generale al cloud da prendere in esame, ad esempio quella relativa alla *data minimisation*, ossia alla riduzione al minimo dei dati e dei trattamenti. Il cloud, in effetti, per sua stessa natura tende a lavorare sul principio opposto, quello della ridondanza delle informazioni. Il problema esiste ma non va enfatizzato e probabilmente anche in questo caso il migliore approccio e le migliori soluzioni sono da cercarsi in ambito tecnico, prima ancora che giuridico. In ogni caso, anche sotto un profilo squisitamente giuridico, la ridondanza dei dati non rappresenta a priori un aspetto necessariamente negativo, posto che la ragione della duplicazione delle informazioni risponde anche a logiche di integrità e conservazione delle medesime. Lo stesso D. Lgs. 196/2003 - Codice in materia di protezione dei dati personali ("Codice Privacy") prevede ad esempio il backup dei dati, ossia una forma di ridondanza dell'informazione, come misura minima di sicurezza da osservare. A ciò si aggiunga che lo stesso Garante per la

protezione dei dati personali ("Garante Privacy"), nella recente "Scheda di documentazione cloud computing: indicazioni per l'utilizzo consapevole dei servizi" [GAR10], sostiene che:

> "(…) nel caso in cui i dati trattati non siano i propri, come avviene per aziende e pubbliche amministrazioni che raccolgono e detengono informazioni di terzi, l'adozione di servizi che non offrono adeguate garanzie di riservatezza e di continuità operativa può avere rilevanti ripercussioni nel patrimonio informativo dei soggetti cui i dati si riferiscono. In tal senso, il titolare del trattamento dei dati a fronte del contenimento di costi dovrà comunque provvedere al salvataggio (backup) dei dati allocati nel cloud, ad esempio creandone una copia locale (eventualmente sotto forma di archivio compresso), allo scopo di gestire gli eventuali rischi insiti nell'acquisizione di servizi che, pur con i vantaggi dell'economicità, potrebbero tuttavia non offrire sufficienti garanzie di affidabilità e di disponibilità."

Anche i D. Lgs. 82/2005 e 235/2010 contengono prescrizioni finalizzate alla continuità operativa e al disaster recovery che presuppongono forme di ridondanza dei dati. Le linee guida [DIG11] emesse da DigitPA a seguito dei decreti citati approfondiscono alcuni degli aspetti tecnici e contrattuali delle soluzioni, anche di tipo cloud, idonee a garantire la continuità del funzionamento delle organizzazioni pubbliche.

È semmai corretto perciò impostare il problema in un'ottica di bilanciamento tra esigenze di preservazione del dato, assolte dal ricorso alla ridondanza, ed esigenze di minimalismo informativo. Esiste verosimilmente un quantum desiderabile di ridondanza su cui ci può attestare strutturando in maniera consapevole gli strumenti tecnologici utilizzati.

Va notato comunque che il principio della data minimisation assume un significato particolarmente cogente in ambito pubblico e rispetto ad alcune tipologie di dati (dati sensibili e giudiziari), per applicazione dell'art. 22, commi 3 e 5 Codice Privacy, e che dunque il problema si pone quale passaggio non secondario cui dedicare specifici approfondimenti.

PROBLEMATICHE DI SICUREZZA

Rimandando ai numerosi riferimenti citati per approfondimenti di tipo generale su cloud e sicurezza, la presente analisi si concentra sullo scenario quello di una PA in veste di consumer di servizi cloud. Tale semplificazione è stata introdotta sulla base dei seguenti presupposti:

- la maggior parte dei rischi e dei benefici per la sicurezza introdotti dal cloud e individuati nel documento sono i medesimi per cloud consumer e cloud provider;
- le *best practice* suggerite sono strumenti di supporto sia per il CSC che per il CSP;
- la creazione di un cloud privato o di comunità per la pubblica amministrazione, pur dovendo basarsi sui criteri generali di sicurezza menzionati nel presente documento, richiede un studio ad hoc al fine individuare nel dettaglio requisiti e criticità.

In termini generali, le pubbliche amministrazioni devono avvicinarsi ai servizi cloud privilegiando atteggiamenti orientati alla prudenza e alla consapevolezza come suggerito, tra gli altri, dal Garante per la protezione dei personali [GAR10] ed ENISA [ENISA09][1]. Entrambe le istituzioni raccomandano un'attenta valutazione dei rischi legati alla fruizione di servizi IT in modalità cloud computing al fine di preservare confidenzialità e integrità dei dati dei cittadini, l'integrità e la continuità dei servizi loro offerti, il loro diritto alla privacy ed infine e più in generale l'interesse e la sicurezza nazionale.

L'adozione di servizi cloud ha una grande attrattiva per i potenziali CSC per i vantaggi in termini di costo, flessibilità, elasticità e agilità, ma nel contempo, suscita anche preoccupazioni, legate a rischi, in alcuni casi reali o in altri solo

[1] Cfr. anche [CON11].

percepiti, riguardo la capacità dei CSP di offrire adeguati livelli di protezione dati e delle applicazioni, controllo, affidabilità, trasparenza e conformità legale.

POTENZIALI RISCHI PER LA SICUREZZA

Alcuni rischi per la sicurezza del cloud sono presenti anche in altre tipologie di outsourcing mentre altri sono legati a questa specifica modalità di erogazione. Tra i principali criticità/rischi che i CSC devono affrontare si possono ricordare [ENISASR09]:

- *Loss of governance*: quando il cliente necessariamente cede il controllo al fornitore di una serie di aspetti che impattano le difese di sicurezza.
- *Lock-in*: al momento attuale il modo in cui si fruisce dei servizi cloud e l'immaturità o l'assenza di strumenti, standard e formati di dati interoperabili rende difficile migrare da un fornitore ad un altro.
- *Isolation failure*: per ottenere le necessarie economie di scala il cloud provider deve mettere in comune le risorse tra più clienti e consentirne l'accesso per la sola parte di specifica competenza (isolation). Esiste quindi la possibilità che per un attacco o per un errore tale separazione venga meno compromettendo la riservatezza.
- *Compliance risks*: ci sono situazioni in cui la compliance a leggi e regolamenti non è possibile tramite soluzioni cloud. Inoltre può capitare che il fornitore non possa fornire evidenza della propria compliance o non permettere audit da parte del cliente.
- *Management interface compromise*: l'accesso alle interfacce di gestione del public cloud da parte dei clienti deve necessariamente avvenire tramite Internet e fornisce un maggior controllo rispetto alle soluzioni di hosting. Tale capacità però comporta un aumentato rischio per il cliente nel caso di vulnerabilità e attacchi.
- *Data protection*: il cloud computing presenta molti rischi relativi alla protezione del dato. Può essere difficile per il cliente controllare che i dati siano utilizzati legalmente. Il problema è esacerbato nel caso di cloud federati (con trasferimenti multipli di dati) e con l'ampliarsi delle catene di subfornitura.
- *Insecure or incomplete data deletion*: quando viene fatta una richiesta di cancellare una risorsa, come spesso accade nei sistemi operativi, essa può essere rimossa ma non effettivamente distrutta e resa irrecuperabile. Tale situazione che include anche i casi di distruzione dei supporti fisici da dismettere e le copie di backup, è oggettivamente più complessa nel caso di ambienti cloud multi cliente che condividono hardware e software.
- *Malicious insider*: i danni che il personale interno all'organizzazione fa quando adotta comportamenti illeciti, sono molto elevati anche se numericamente meno frequenti degli attacchi dall'esterno. Ci sono persone nell'organizzazione che ricoprono ruoli estremamente delicati, come ad esempio gli amministratori di sistema. Un fornitore (ed un cliente) di servizi cloud non possono esimersi dal considerare questo rischio in tutte le sue implicazioni.

POTENZIALI VANTAGGI PER LA SICUREZZA

Come evidenziato da analisi condotte da ENISA, il modello cloud è in grado di offrire alle organizzazioni pubbliche benefici dal punto di vista della sicurezza dovute in particolare a:

- specializzazione del personale e presenza di strutture dedicate che permettono soluzioni di sicurezza di maggior qualità rispetto a quelle consuete;
- migliori soluzioni per la business continuity e disaster recovery (ridondanza geografica, edge networks, riallocazione dinamica delle risorse, tolleranza ad attacchi, etc);
- maggiore efficienza ed efficacia nei processi di change management, patch management, hardening, incident management, security assessment e security testing.

Non bisogna dimenticare, infatti, che la sicurezza in ambito cloud deve essere valutata in relazione alle soluzioni che i clienti di servizi cloud avrebbero potuto realizzare al proprio interno con le risorse a loro disposizione. Infatti i CSP,

potendo fare leva sulle economie di scala, sono in grado di realizzare soluzioni molto più evolute rispetto a quelle che sono, di norma, implementabili dai CSC su una molteplicità di realizzazioni di minori dimensioni.

Le caratteristiche delle soluzioni cloud possono, ad esempio, consentire di:

- realizzare architetture ridondate e geograficamente distribuite;
- scalare risorse per rispondere a eventuali attacchi di tipo DDoS;
- utilizzare servizi di monitoraggio evoluti;
- ridurre i tempi di reazione agli incidenti;
- realizzare soluzioni di sicurezza fisica più robuste;
- integrare l'organizzazione della sicurezza nei CERT e con le forze di polizia;
- assicurare maggiore omogeneità e coerenza delle varie soluzioni di sicurezza.

Infine, dovendo rivolgersi a molteplici soggetti diversi, i CSP hanno la necessità di orientare i propri servizi verso modalità di erogazione standard e, qualora possibile, aperte. Ciò comporta, dal punto di vista della sicurezza, una tendenza a convergere su soluzioni standard e aperte con indubbi riflessi positivi sulle capacità di controllo ed esecuzione.

2.4 Infrastrutture tecnologiche

Nella PA centrale vi sono più di 1000 data center di diverse dimensioni distribuiti sul territorio, che ospitano più di 20.000 server e oltre 3 milioni di punti-funzione di software proprietario, per un costo annuo complessivo per la sola gestione di 450 milioni di euro [CNI08]. Questi data center sono spesso duplicati nelle funzioni e privi di una visione sistemica attraverso la quale attuare sinergie basate sulla standardizzazione, l'interoperabilità, l'evoluzione tecnologica, la condivisione delle risorse e strategie di acquisto coordinate.

L'inefficienza e la stratificazione tecnologica prodotta da uno scenario del genere sono evidenti. Si pensi alle tante funzioni duplicate, soprattutto quelle di back office, alla duplicazione dei servizi di gestione, al sotto-utilizzo delle risorse informatiche, agli spazi fisici, ai consumi energetici necessari per alimentare gli apparati IT e soprattutto gli apparati di condizionamento, alla frammentazione dei contratti con i fornitori che riduce fortemente il potere negoziale e le economie di scala.

Questa realtà, oltre ad assorbire ingenti risorse economiche, rappresenta un ostacolo per l'introduzione di tecnologie e servizi ad alto valore che contribuirebbero all'innovazione della Pubblica Amministrazione e del sistema Paese nel suo complesso.

È necessario avviare un circolo virtuoso che liberi i costi che non generano valore e permetta investimenti in servizi ad alto impatto per i cittadini e la collettività. Il modello cloud può consentire di innescare questo circolo virtuoso e recuperare l'efficienza della PA.

Una prima opportunità in questo senso sarebbe offerta dall'avvio di un programma di razionalizzazione delle infrastrutture tecnologiche che, altre ad essere di grande valore in sé, faciliterebbe anche l'introduzione del modello del cloud computing su larga scala. Il programma di razionalizzazione potrebbe iniziare con uno studio, guidato da DigitPA e con la partecipazione dalle amministrazioni coinvolte, che analizzasse i modelli di razionalizzazione possibili valutando i percorsi, le architetture tecnologiche, le modalità di realizzazione, gli impatti organizzativi, il ritorno degli investimenti ed i benefici ottenibili.

Una seconda opportunità proverrebbe dal favorire ed indirizzare l'acquisizione di servizi cloud da parte delle singole Amministrazioni, alle quali dovrebbe essere richiesto, nell'ambito dei loro bandi di gara, di valutare anche i servizi cloud, in maniera similare a quanto prevede la normativa vigente per il software open source.

Mediante l'adozione di servizi in cloud è possibile, per un amministrazione, riposizionare l'organizzazione IT da gestore del sistema a gestore del servizio, potenziando le conoscenze di processo ed applicative piuttosto che quelle tecnologiche e di prodotto.

Uno dei nuovi compiti dell'organizzazione IT dovrebbe essere quello di individuare tra le offerte disponibili quelle che possono aumentare la produttività dell'amministrazione, di agevolare il loro percorso di inserimento nei processi amministrativi e favorirne l'adozione.

L'adozione del modello dovrebbe comportare, in molti casi, l'integrazione dei processi delle pubbliche amministrazioni anche mediante l'unificazione delle banche dati.

La possibilità di fruire di servizi applicativi innovativi, ora impensabili a causa degli ingenti investimenti tecnologici richiesti, favorirebbe lo snellimento di molte procedure, per un servizio più efficiente verso il cittadino.

In un modello cloud privato interno, l'amministrazione che fruisce di servizi cloud deve mantenere in linea di massima le competenze tradizionali per la gestione dei dispositivi di accesso e acquisire quei cloud necessari alla corretta fruizione dei servizi e all'integrazione con l'ambiente IT tradizionale.

La fruizione di un servizio da un cloud pubblico generalmente richiede meno competenze IT poiché le infrastrutture e le relative problematiche di gestione sono a cura del provider. Anche in questo modello le competenze IT sono necessarie se vi sono scenari di integrazione con infrastrutture esistenti.

Poiché la PA presenta una presenza capillare sul territorio, è molto probabile che essa tenda analogamente verso una dispersione di tecnologie e dati, ricorrendo nella scelta delle soluzioni cloud a più service provider per la stessa esigenza.

Il pericolo per l'amministrazione potrebbe quindi essere un eccessivo *overhead* contrattuale e gestionale dovuto alla molteplicità di interfacce e di tecnologie, soprattutto nel caso l'amministrazione decida di mantenere al suo interno una parte delle attività di gestione IT.

Quanto fin qui esposto si applica nei casi in cui un'amministrazione si trovi nell'eventualità di dover erogare un nuovo servizio o di dover adeguare la propria infrastruttura e sia per le dimensioni sia per l'onere che ne deriva, decide di avvalersi di soluzioni di tipologia cloud, con i vincoli che questa scelta non implichi una rinuncia di strategia né diventi un ostacolo al raggiungimento dei propri obiettivi.

3. CONDIZIONI DI SUCCESSO DI INIZIATIVE CLOUD

Come si è visto nel precedente capitolo, l'adozione dei servizi cloud presenta rilevanti vantaggi ma anche numerosi rischi rispetto ai quali al momento non esistono soluzioni generali. Per questo motivo, in questo capitolo vengono evidenziati i fattori di successo più utili per contrastare e, in alcuni casi, per annullare i rischi riconosciuti in ciascuno degli ambiti esaminati nel documento.

3.1 ASPETTI GENERALI

È molto diffusa l'opinione che, a causa del particolare contesto informativo, organizzativo e giuridico, l'adozione dei servizi cloud da parte della pubblica amministrazione italiana debba necessariamente essere lenta e difficoltosa. A parte una ragionevole dose di prudenza, del resto applicabile ad ogni altro paradigma innovativo, si ritiene utile adottare un atteggiamento pragmatico ma costruttivo, anche su temi come la sicurezza o la *privacy* attorno ai quali in un primo momento si erano raccolte le maggiori preoccupazioni.

Pur in un quadro in rapida evoluzione, i servizi cloud si presentano come uno dei mezzi più economici per assicurare ad una gran parte dei servizi di eGovernment caratteristiche di efficacia, efficienza, trasparenza, partecipazione, condivisione, cooperazione, interoperabilità e sicurezza. Le strategie di eGovernment di molti Paesi (tra i quali USA, UK, Francia, Giappone e Canada) puntano già con decisione alla promozione e all'adozione del cloud da parte dell'amministrazione statale. Come già ricordato, sono attese durante la primavera del 2012 la pubblicazione di una strategia cloud europea, annunciata dalla VP della Commissione UE Neelie Kroes [KRO11, KRO12], la cui preparazione è stata accompagnata da numerosi studi e approfondimenti tecnici e da una vasta consultazione, e l'avvio della *European Cloud Partnership* [KRO12], che punta a promuovere il *procurement* di servizi cloud a livello europeo concordando requisiti e standard adeguati al settore pubblico.

Mai come in questo campo le attività di sperimentazione, standardizzazione e regolazione vengono svolte secondo un approccio intrinsecamente globale, proprio come intrinsecamente globali sono le offerte commerciali di servizi cloud. Qualunque cammino di adozione del cloud verrà seguito nel nostro Paese, è quindi necessario mantenere una visione e una presenza costanti anche a livello internazionale.

Tra gli effetti dell'adozione dei servizi cloud forse meno immediati ma più promettenti, in particolare per la pubblica amministrazione, si può prevedere il miglioramento del rapporto con l'utente ispirato alla qualità, semplicità e raffinatezza dei servizi online dai quali lo stesso paradigma del cloud ha avuto origine in anni recenti. Le economie di scala alla base del successo di questo modello derivano infatti da una co-ingegnerizzazione spinta di infrastrutture IT, dati ed applicazioni pensata e realizzata attorno all'utente finale. La promessa di ottenere vantaggi analoghi per i servizi pubblici suggerisce di tentare un ripensamento di alcuni aspetti dell'ICT pubblica.

I temi ai quali fare maggiormente attenzione sono la condivisione e la colocalizzazione dei dati, la semplificazione e il riuso delle applicazioni. Il ricorso diffuso da parte della pubblica amministrazione ai servizi cloud, siano essi di tipo pubblico o di tipo privato, porta con sé un superamento delle modalità verticali di gestione e di elaborazione dei dati, rendendo più semplice implementare interfacce standard e riutilizzabili.

3.2 ASPETTI GIURIDICI

L'utilizzo di servizi cloud da parte di una PA non può essere considerato in senso astratto e generico ma va attentamente studiato e calibrato sull'esigenza specifica di trattamento e sulle caratteristiche di quest'ultimo, il che

comporta necessariamente una valutazione preliminare di conformità e una minuziosa predisposizione della stipulazione contrattuale. A tal proposito, nei rapporti contrattuali fra cloud provider e buyer si propone l'impiego di Privacy Level Agreement (di seguito: "PLA"), una sorta di Service Level Agreement (di seguito: "SLA") con riferimento ai livelli/accordi/garanzie di tutela e sicurezza dei dati personali che il cloud provider si impegna a mantenere verso il cliente. Oggetto di tali PLA potranno essere per es:

- specifiche misure di sicurezza sui dati (es. utilizzo di cifratura sia in fase di storage che in fase di comunicazione), comprovate anche da eventuali certificazioni (es. ISO), nonché possibilità e modalità di controllo da parte della PA (es. audit diretto, attraverso terze parti, o report periodica del cloud provider);
- limiti nella circolazione/trasferimento dei dati, sia territoriali (es. che i dati non vengano trasferiti verso paesi fuori dallo SEE nei quali non sia garantito un livello di protezione 'adeguato' agli standard comunitari) che con riferimento ai soggetti coinvolti (es. sub-fornitori del cloud provider principale);
- esplicite garanzie con riferimento al mantenimento di un adeguato livello di tutela dei dati personali non solo da parte degli incaricati e responsabili interni alla struttura del cloud provider ma anche degli eventuali sub-fornitori utilizzati; e tracciabilità delle azioni svolte dai vari soggetti sui dati, al fine di poter ricostruire le relative responsabilità;
- garanzia di data portability e di assistenza in un eventuale procedura di transfer back (in termini di giorni/uomo);
- indicazione delle politiche di persistenza dei dati con riferimento alla loro conservazione (*data retention*).

Il PLA è da intendersi di fatto come un allegato al contratto di fornitura di servizi cloud (proprio come lo SLA). L'eventuale violazione di quanto riportato nel PLA costituirebbe un inadempimento da parte del cloud provider dal quale deriverebbero i relativi effetti contrattuali (es. risoluzione, attivazione penali, risarcimento, ecc.).

Inoltre, con riferimento alla regolamentazione e gestione dell'utilizzo del cloud da parte della PA si raccomanda:

- lo studio di eventuali linee guida di settore che traccino le garanzie minime 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, infatti: (i) chiarirebbe i requisiti minimi che devono essere tenuti in considerazione dai provider nel proporre un'offerta cloud per la PA; (ii) potenzierebbe la forza negoziale della PA al fine di ottenere servizi sempre più rispondenti alle proprie esigenze; e (iii) 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;
- che i prossimi interventi sia a livello europeo che a livello nazionale chiariscano gli obblighi e le responsabilità delle parti coinvolte, possibilmente superando anche formalismi legati a definizioni o ruoli; in attesa di tali riforme o indicazioni, sarà necessario precisare chiaramente nel contratto di fornitura cloud i rispettivi obblighi e responsabilità delle parti, anche con specifico riferimento alla disciplina sulla tutela dei dati personali;
- la definizione di nuove soluzioni per abilitare i trasferimenti di dati in contesti extra-europei, che assicurino una tutela concreta dei dati dei soggetti interessati; stanti i limiti della disciplina attualmente in vigore, pare consigliabile esigere e richiedere garanzie che i dati non vengano trasferiti verso paesi fuori dallo SEE nei quali non sia garantito un livello di protezione adeguato agli standard comunitari.

I *CLOUD SERVICE AGREEMENT*

Ai contratti di cloud computing di una P.A., come del resto a tutti i contratti stipulati da una P.A. italiana con un operatore economico, si rendono applicabili, tra l'altro, sia le disposizioni relative ai contratti pubblici contenute nel Codice degli appalti pubblici e nel relativo Regolamento, sia le disposizioni sul contratto presenti nel codice civile.

Al riguardo si osserva che, da una preliminare ricognizione operata da DigitPA su un limitato campione di contratti di cloud, risulta che attualmente tali servizi verrebbero offerti proponendo ai clienti, anche se Pubbliche Amministrazioni,

la sottoscrizione di contratti c.d. “per adesione” dove le clausole contrattuali risultano a scarsa (o nulla) negoziabilità. Tali strumenti contrattuali sono in effetti predisposti in via prevalente per un’utenza di tipo privato (società o privati cittadini) e quindi, sovente, non risultano del tutto coerenti con la vigente normativa che disciplina gli appalti pubblici di servizi.

Si ritiene, di conseguenza, utile evidenziare di seguito quali sono le clausole contrattuali che è opportuno inserire in un contratto di cloud.

In via preliminare si osserva che, posto che si ritiene (come precedentemente evidenziato) il contratto di cloud computing rientrante tra i contratti di appalto di servizi, risulta interessante soffermarsi brevemente sulla causa contrattuale, che fa parte dei requisiti che il codice civile prevede in generale per il contratto .

In particolare il contratto di cloud computing, in quanto contratto di appalto pubblico di servizi, ha la sua causa nell’erogazione del servizio richiesto rispettando gli SLA minimi pattuiti e ritenuti essenziali verso il pagamento del corrispettivo pattuito. Ne consegue che qualora il contratto non preveda un’obbligazione di risultato a carico dell’operatore economico aggiudicatario (ad esempio in caso di contratto di SaaS-cloud l’operatore economico non assicuri alla P.A. la fruizione con degli SLA minimi delle applicazioni messe a disposizione nell’infrastruttura cloud ma si preveda una fruizione “as is” – ovvero “così com’è”) verrebbe meno la causa contrattuale (in pratica viene meno l’interesse della PA ad utilizzare i servizi di cloud per i quali l’operatore economico non si assuma l’obbligo di rispettare SLA minimi ritenuti essenziali e cade quindi la giustificazione del correlato obbligo del pagamento del corrispettivo) e ne deriverebbe la nullità del contratto medesimo per mancanza appunto della causa.

Si formulano alcune considerazioni limitatamente a clausole che in un contatto di cloud computing è opportuno valutare con particolare attenzione.

LE CLAUSOLE CONTRATTUALI

La stazione appaltante dovrà definire, sia nello schema di contratto che nel disciplinare di gara e nel capitolato tecnico, quali sono le caratteristiche del servizio che si intende acquisire e le modalità di esecuzione delle prestazioni contrattuali. Lo schema di contratto dovrà perseguire una serie di finalità volte a tutelare la PA rispetto a tutti i rischi connessi all’utilizzazione di contratti standard proposti in materia di cloud.

In particolare, nella documentazione contrattuale e nell’offerta il fornitore deve garantire, pena la risoluzione per inadempimento con escussione della garanzia fideiussoria prestata fatti salvi ulteriori danni, la presenza sul territorio italiano o nell’ambito dell’UE dell’infrastruttura utilizzata per l’erogazione dei servizi di cloud precisando, in caso di infrastrutture presenti in ambito UE, che al contratto dovrà comunque essere applicata la legge italiana e che in caso di controversia l’autorità giudiziaria competente a conoscere della questione sarà comunque quella italiana.

Apposite previsioni contrattuali dovranno disciplinare gli standard ed i livelli di servizio necessari alla corretta esecuzione del contratto stesso.

In particolare, anche in ragione dell’innovatività delle iniziative in esame e del carattere sperimentale delle modalità di fornitura di servizi cloud, occorrerà introdurre un adeguato sistema di monitoraggio – al quale dovrà essere sottoposta l’attività del fornitore – che consenta il riscontro e la verifica continua delle attività svolte e dei servizi resi. Per tale ragione il fornitore dovrà essere nelle condizioni di predisporre adeguata reportistica delle attività rese.

Il contratto dovrà poi prevedere penali contrattuali per la violazione di qualsiasi standard qualitativo che la prestazione debba assicurare.

Quanto agli obblighi che specificamente dovranno essere a carico del fornitore, sarà opportuno prevedere:

- l'oggetto contrattuale dovrà essere puntualmente definito indicando e quantificando esattamente quali sono gli specifici impegni assunti dal fornitore in fase di avvio, esecuzione e conclusione del contratto , rinviando al capitolato tecnico per quanto riguarda le relative specifiche tecnico-informatiche;
- i livelli di servizio e le relative penali. In considerazione della tipologia di servizi gli SLA dovranno, tra l'altro, definire con attenzione gli aspetti relativi alle esigenze di assicurare un'elevata continuità nell'erogazione dei servizi che garantisca la PA riguardo la propria continuità operativa. In merito alle penali occorre precisare che la violazione dei livelli di servizio e gli inadempimenti in generale (mancato raggiungimento della qualità prevista nell'offerta tecnica dunque nel contratto) devono essere puntualmente disciplinati;
- verifiche con periodicità breve (ad es. mensile), anche tramite l'utilizzazione di appositi applicativi informatici messi a disposizione del fornitore, del corretto adempimento delle prestazioni eseguite dal fornitore stesso, da prevedere con clausole contrattuali coerenti con quanto previsto dalle vigenti disposizioni relative alla verifica di conformità;
- la previsione di procedure di gestione degli eventi imprevedibili che possano incidere sulla tempestività e sulla qualità delle prestazioni rese (con adeguata registrazione degli eventi stessi);
- la definizione di sistemi adeguati che intervengano in caso di malfunzionamento per evitare o limitare al massimo qualsiasi tipo di interruzione del servizio;
- la predisposizione di sistemi di sicurezza idonei a garantire la sicurezza dei dati della PA; il sistema dovrà prevedere modalità di recupero e conservazione dei dati sia in caso di disservizio;
- garantire la sicurezza dei dati e assicurare sempre la titolarità degli stessi;
- inquadrare correttamente la responsabilità del fornitore verso la PA;
- assicurare le integrazioni con i sistemi SW già in uso presso la PA;
- prevedere specifici impegni del fornitore per quanto riguarda le attività di affiancamento con il fornitore subentrante a seguito di una nuova aggiudicazione o anche in caso di risoluzione per inadempimento del fornitore o recesso anticipato da parte della PA.

Occorre quindi considerare che le disposizioni contenute nella documentazione che disciplinerà il contratto di cloud devono, ovviamente, risultare coerenti anche con quelle del regolamento attuativo (DPR. n. 207/2010) del Codice degli Appalti pubblici, dove, ad esempio, l'art. 298 prevede che i contratti precisino le penali da applicare nel caso di ritardato adempimento degli obblighi contrattuali, in relazione alla tipologia, all'entità ed alla complessità della prestazione, nonché al suo livello qualitativo.

Rispetto al riscontro del corretto adempimento delle prestazioni eseguite, la stazione appaltante dovrà attentamente disciplinare la verifica di conformità .

Le prestazioni oggetto di contratto di cloud computing rientreranno tra quelle di cui all'articolo 300, comma 2, lettera b) del citato Regolamento, e cioè prestazioni particolarmente complesse sotto il profilo tecnologico, ovvero, che richiedono l'apporto di una pluralità di competenze ovvero caratterizzate dall'utilizzo di componenti o di processi produttivi innovativi o dalla necessità di elevate prestazioni per quanto riguarda la loro funzionalità.

Per questo la stazione appaltante attribuirà l'incarico della verifica di conformità ad un soggetto o ad una commissione composta da due o tre soggetti che siano in possesso della competenza tecnica eventualmente necessaria in relazione all'oggetto del contratto (art. 314, c. 2, del Regolamento).

Alla luce delle particolarità delle prestazioni e della necessità di verificare l'esatta esecuzione, dunque tenuto conto della natura delle prestazioni, del contenuto del contratto e di ogni altra circostanza le stazioni appaltanti potranno decidere, come si ritiene opportuno, di procedere a verifica di conformità in corso di esecuzione al fine di accertare la piena e corretta esecuzione delle prestazioni contrattuali, con la cadenza adeguata per un accertamento progressivo della regolare esecuzione delle prestazioni (art. 313 c. 3 del Regolamento).

A sua volta il capitolato tecnico dovrà tra l'altro:

- prevedere tutti gli aspetti e le caratteristiche tecniche, funzionali ed operative della fornitura,
- indicare gli standard tecnici richiesti ;
- descrivere precisamente gli obiettivi da perseguire ed i servizi da acquisire;
- richiedere la compatibilità con prodotti informatici già in uso presso la PA;
- pretendere la realizzazione di una modalità esecutiva o di un progetto o di un sistema che consenta con facilità il passaggio se del caso ad altro fornitore.

3.3 Privacy e sicurezza

Ad un livello di maggiore approfondimento, si propone qui una rassegna degli elementi di maggiore rilevanza nelle scelte che la PA è chiamata ad operare quando valuta la migrazione dei dati in una struttura cloud.

Allocazione dei ruoli

L'allocazione dei ruoli rappresenta uno degli aspetti più delicati, non solo in materia di cloud ma nella complessiva applicazione della disciplina sulla tutela dei dati personali. Posto che la PA che acquista servizi di cloud va senz'altro considerata titolare di trattamento, il problema si pone dal lato del cloud provider che potrebbe, a seconda dei casi, essere considerato quale titolare autonomo di trattamento o quale responsabile. Va evidenziato che, stante la vigente normativa sulla tutela dei dati personali, parrebbe ragionevole orientarsi per la soluzione della titolarità autonoma in base a tutta una serie di ragioni che qui potremo solo accennare ma che sono state analizzate nel dettaglio recentemente in [IIPP11]. Tuttavia, la prassi che si riscontra negli accordi per la fornitura di servizi cloud è di definire il cloud provider un responsabile esterno del trattamento. Anche la soluzione del cloud provider come responsabile esterno del trattamento appare di fatto prospettabile, dipendendo in definitiva il concreto inquadramento nell'una o nell'altra dalle caratteristiche dell'effettivo rapporto che si instaura tra buyer e provider.

In estrema sintesi, il "titolare del trattamento è sostanzialmente colui che prende le decisioni quanto alle finalità del trattamento (ossia il perché del trattamento), alle modalità essenziali e al profilo della sicurezza. (…) Si può da subito evidenziare che il cloud provider ha un ruolo esclusivo, rispetto al buyer, sulla decisione del profilo della sicurezza e sulla modalità di erogazione del proprio servizio, incluse le scelte relative alla circolazione dei dati nei diversi luoghi e tra distinti soggetti", come suoi subfornitori.

Il responsabile è "individuato dalla caratteristica essenziale di agire sempre nel perimetro delle decisioni del titolare e sotto la direzione e vigilanza di costui. Sul punto è bene evidenziare che vi è un preciso obbligo giuridico del titolare di impartire disposizioni scritte analitiche al responsabile (art. 29, c. 4 Codice), che potranno essere modificate e aggiornate nel tempo a discrezione del primo: ciò comporta, implicitamente, un dovere del responsabile di rispettare ed attenersi precisamente alle istruzioni del titolare, caso, quest'ultimo decisamente inverosimile quando si parla di un grande cloud provider, da un lato, e di una piccola e media impresa-buyer, dall'altro." Tuttavia, ad oggi risulta verosimile asserire che, nella maggior parte dei casi, nemmeno buyer come una grande impresa o una PA riescano di fatto ad impartire istruzioni dettagliate al cloud provider e ad esercitare quel controllo tipico del rapporto titolare-responsabile. Quindi, la soluzione di fatto più aderente alla normativa privacy odierna è quella di una titolarità autonoma del cloud provider.

Le conseguenze dell'allocazione dei ruoli sono notevoli e si riflettono su tre ordini di questioni: (i) individuazione della legge nazionale applicabile; (ii) definizione della responsabilità giuridica e dei poteri di accesso e controllo tra le parti; (iii) individuazione della disciplina specifica applicabile al trattamento.

Quanto al primo profilo va ricordato che, a norma dell'art. 5 del Codice Privacy letto alla luce dell'art. 4 della Direttiva 95/46/CE, è innanzitutto lo stabilimento del titolare a determinare l'individuazione della legge nazionale applicabile. Quindi, individuare se un cloud provider è titolare o responsabile ha conseguenze evidentemente decisive sulle norme applicabili in concreto.

Quanto al secondo profilo, va ricordato che alla posizione apicale del titolare è associata una corrispondente responsabilità giuridica e che, per necessaria conseguenza, proprio a fronte di questa posizione di vertice e della connessa responsabilità, il titolare esercita e deve esercitare penetranti poteri di controllo e di pretesa di rendiconto sul responsabile (ex art. 29 Codice Privacy).

Infine, quanto al terzo profilo, deve evidenziarsi che la trasmissione di dati ad altro titolare integra un'operazione di comunicazione: ove il destinatario sia un soggetto privato e i dati siano dati comuni, è necessario ai sensi dell'art. 19, c. 3 Codice privacy il supporto di apposita norma di legge o di regolamento.

La presente incertezza di fatto sull'individuazione dei ruoli privacy impedisce di operare un'accurata valutazione del rischio legale e quindi di prendere una decisione informata circa la migrazione verso il cloud. Se tale situazione può essere gestita nel settore privato, dove esiste una maggiore propensione al rischio, nel settore pubblico – si pensi ad esempio a servizi sanitari – tale rischio non è sostenibile. Esistono infatti procedure di controllo e governo dei dati molto dettagliate e stringenti, soprattutto con riferimento a quelli idonei a rivelare lo stato di salute.

Occorre quindi che i prossimi interventi sia a livello europeo che a livello nazionale chiariscano gli obblighi e le responsabilità delle parti coinvolte, magari superando l'attuale approccio fondato su formalismi legati a definizioni astratte. Nelle more di nuove indicazioni, che si auspica possano precisare le diverse fattispecie di ruoli preordinati, andrà dedicata in ciascun caso specifico nel contratto di fornitura cloud particolare attenzione alla specifica dei rispettivi obblighi e responsabilità delle parti, anche con specifico riferimento alla disciplina sulla tutela dei dati personali.

INDIVIDUAZIONE DELLA TIPOLOGIA DI DATI DA MIGRARE

Altro elemento fondamentale sul quale concentrare l'attenzione è l'esatta individuazione della tipologia di dati da migrare sul cloud: comuni, sensibili (e tra questi i dati sanitari), giudiziari. In via generale deve evidenziarsi che il passaggio al cloud va calibrato sulla specie del trattamento eseguito.

Nel caso dei dati comuni, ove il cloud provider sia un soggetto privato titolare autonomo di trattamento, occorre che la PA, che in qualità di buyer comunica i dati, operi sulla base di una norma di legge o di regolamento. Qui non può sottacersi che, mentre sul versante della predisposizione di regolamenti in materia di trattamento dei dati sensibili, adottati su parere del Garante Privacy ai sensi dell'art. 20 Codice Privacy, si è lavorato molto, raggiungendo nella sostanza l'obiettivo di colmare le lacune esistenti, gli enti che si sono dotati di un proprio regolamento per la comunicazione/diffusione dei dati personali comuni sono invece assai pochi, data anche la difficoltà obiettiva di censire questi ultimi, specie in organizzazioni di una certa complessità. Il problema assume perciò anche una dimensione pratica da tenere presente, che peraltro trascende i confini del tema cloud.

Quanto ai dati sensibili, occorre la presenza di una norma di legge o di regolamento, mentre va escluso che il conferimento dei dati personali in un cloud possa costituire di per sé una speciale operazione di trattamento, diversa da una normale comunicazione a un titolare autonomo o da una trasmissione ad un responsabile, e come tale da normare in maniera apposita nella fonte primaria o secondaria.

Discorso sostanzialmente analogo vale per i dati giudiziari, secondo la regola generale di cui all'art. 21 Codice Privacy, che per la liceità del trattamento richiede l'espressa disposizione di legge o il provvedimento del Garante Privacy.

Piuttosto, occorrerà curare da parte dell'amministrazione fruitrice che sia rispettata nel cloud la regola di cui all'art. 22, c. 6 Codice Privacy sull'utilizzo di tecniche di cifratura o che rendano temporaneamente inintelligibile il dato. Ciò naturalmente è tanto più vero nel caso in cui cloud provider sia responsabile di trattamento, e come tale si collochi entro la struttura del titolare PA, ma non è da escludere che trovi applicazione – magari attraverso opportuni strumenti contrattuali – anche quando la PA affida i dati a un privato titolare autonomo di trattamento. Il problema della cifratura e dell'inintelligibilità incontra comunque soddisfacenti soluzioni di tipo tecnico-informatico, e appare affrontabile con

esito positivo in quell'ambito, a patto naturalmente che il cloud provider non abbia accesso ai codici di cifratura e sia possibile trovare tra gli interpreti accordo sul tipo di cifratura considerato adeguato.

INDIVIDUAZIONE DELL'AMBITO DI TRATTAMENTO

Un terzo elemento fondamentale sul quale porre l'attenzione è rappresentato dall'ambito al quale si riferisce il trattamento. Per affrontare immediatamente situazioni complesse, si può fare l'esempio dell'ambito sanitario, dove esiste una stringente disciplina di settore da tenere presente.

Questo passaggio si interseca peraltro con il precedente, relativo alla corretta identificazione dei dati, in quanto i dati idonei a rivelare lo stato di salute sono disciplinati da disposizioni specifiche. Di particolare importanza è il principio di separazione dagli altri dati personali, ai sensi dell'art. 22, c. 7 Codice Privacy. Sul punto si può ripetere quanto già osservato in termini di cifratura, del resto da osservare strettamente anche in ambito sanitario.

Requisito essenziale in materia di trattamento in ambito sanitario è costituito poi dalla necessità – del tutto eccezionale nel contesto pubblico – di raccogliere il consenso dell'interessato, quale condizione di liceità del trattamento. Una manifestazione di consenso ulteriore, in applicazione delle regole generali, dovrebbe poi essere effettuata dall'interessato anche a proposito del trattamento consistente nella comunicazione ai cloud provider, ove questi siano considerati titolari autonomi, affinché svolgano le operazioni di trattamento consistenti nella registrazione e nella conservazione dei dati all'interno del cloud. Tuttavia sul punto, salvo diverse conclusioni ad esito di approfondimenti specifici, deve ritenersi applicabile la disciplina in materia di semplificazione e, nella specie, l'art. 81 Codice Privacy, che rende possibile l'espressione di un consenso unico e omnicomprensivo.

Ugualmente, l'informativa può essere resa in modo unitario, possibilità del resto sempre ammessa anche in ambiti diversi da quello sanitario. Sembra necessario che l'informativa dia conto del fatto che il dato sarà trattato in un contesto di cloud e contenga una sintetica esposizione delle caratteristiche che ciò comporta.

Aspetto più controverso è se si debba dare conto nell'informativa, anche eventualmente attraverso il richiamo a separato documento accessibile all'interessato, della specifica composizione della 'nuvola', ossia elencare i cloud partner (subfornitori) che ne fanno parte. Tale problema è in realtà avvertito maggiormente nel caso di cloud provider che sia responsabile di trattamento, come tale impossibilitato allo stato, e salvo aperture in senso diverso, dal nominare direttamente altri responsabili, con la conseguenza che – stante la vigente normativa – dovrà necessariamente essere il buyer a designare direttamente questi ultimi.

C'è un ulteriore aspetto, collegato a quest'ultimo, che merita approfondimento e al quale bisogna fare cenno: si tratta della possibilità che il carattere dinamico e non necessariamente determinato a priori della composizione del cloud possa avere ricadute sulla distinzione tra comunicazione e diffusione del dato, con conseguenze rilevantissime, attesa l'illiceità della diffusione dei dati sanitari. Si tratta di tema al quale dedicare approfondimenti specifici, impossibili in questa sede.

Da ultimo, sempre a proposito di trattamento in ambito sanitario, va evidenziato che campo di applicazione particolarmente fertile del cloud si presenta quello della gestione del fascicolo sanitario elettronico. Il grado di complessità e di implicazioni è particolarmente elevato e richiede una trattazione specifica. Qui si può solo rilevare da un lato che il cloud si presenta come una tecnologia particolarmente vantaggiosa nella gestione del fascicolo sanitario elettronico, sia sotto il profilo del contenimento della spesa, sia sotto quello dell'efficienza, dell'interoperabilità e dell'implementazione di stringenti misure di sicurezza, e che dall'altro lato il trattamento deve attestarsi ad un livello particolarmente rigoroso di rispetto delle regole fondamentali in materia di tutela dei dati personali: stretta aderenza alla finalità, pertinenza e non eccedenza, durata limitata del trattamento (compatibilmente con le finalità), rispetto della dignità dell'interessato e dei suoi familiari, corretta e completa informativa, pieno controllo da parte dell'interessato sui propri dati. Tra i vari aspetti tecnologico-giuridici si segnala come il rigoroso controllo degli accessi logici, l'accurata gestione delle identità e dei relativi privilegi al trattamento dei dati, nonché la conservazione

dell'integrità dei medesimi risultano condizioni necessarie per la migrazione – a norma di legge – verso il cloud di tali servizi.

INDIVIDUAZIONE DI MASSIMA DELLA COMPOSIZIONE E STRUTTURA DEL CLOUD

Altro passaggio di rilievo da affrontare in questa rapida rassegna sulle ragioni giuridiche che devono presiedere alla scelta della migrazione al cloud da parte della PA riguarda la verifica, almeno per grandi linee, della composizione della 'nuvola'. E' importante da parte della PA soffermarsi quantomeno sugli aspetti emergenti di maggior rilievo della struttura di cloud scelta, considerando per esempio se si tratta di servizi cloud erogati da soggetti privati o se viceversa non si tratti di servizi cloud erogati da PA o se venga in essere una combinazione intermedia tra questi due modelli. Le ricadute sono a vario livello. Il più immediato, ma non unico, potrebbe essere (a seconda dei casi) quello del rispetto del principio di cui all'art. 19, comma 3 Codice Privacy quanto alla comunicazioni di dati comuni a soggetti privati – ammesse unicamente quando sono previste da una norma di legge o di regolamento.

AMBITO DI CIRCOLAZIONE DEI DATI

Quinto decisivo elemento sul quale porre l'attenzione riguarda infine l'ambito di circolazione dei dati, e più precisamente l'ambito territoriale di trasferimento dei medesimi. Com'è noto l'Unione europea, allargata ai paesi dello Spazio economico europeo (di seguito: "SEE"), costituisce un bacino da considerare in senso unitario. Le complessità reali sorgono invece in occasione di trasferimenti di dati personali in contesti extra-europei nei quali non sia garantito un livello di protezione 'adeguato' agli standard comunitari. Esistono in questo senso strumenti appositi per rendere possibile il trasferimento, quali: (a) il consenso dell'interessato, (b) le Model Clause approvate dalla Commissione europea , (c) le Binding Corporate Rules (di seguito: "BCR") , (d) in caso di data importer statunitense lo strumento del Safe Harbor . In questa sede non è possibile un'analisi di dettaglio dei sopracitati mezzi di trasferimento dati, per un approfondimento sul tema si rinvia al position paper dell'Istituto Italiano per la Privacy 'Cloud computing e tutela dei dati personali in Italia: una sfida d'esempio per l'Europa' al quale si rimanda per un eventuale approfondimento. Per quanto rileva ai fini del presente documento, si sottolinea come questi mezzi per eseguire il trasferimento dati verso paesi fuori dallo SEE nei quali non sia garantito un livello di protezione 'adeguato' agli standard comunitari, non risultino adatti a supportare i trasferimenti multipli di dati tipici della struttura ad architettura distribuita del cloud. Indichiamo brevemente le macro criticità dei vari mezzi di trasferimento dati:

a) il consenso deve essere ottenuto da tutti i soggetti interessati coinvolti (criticità) a valle di un'informativa che dovrà indicare, tra le altre, il tipo di trattamento, la sfera di circolazione (trasferimento, comunicazione e/o diffusione), l'individuazione precisa del paese di destinazione (criticità), nonché le modalità di trattamento dei dati. Inoltre, il consenso può essere in ogni momento revocato dall'interessato e ciò può avere impatti pratici di difficile gestione nel cloud;

b) le Model Clause sono valide unicamente tra i due contraenti (cd. schema point to point). Il fatto che non sia prevista la stipulazione di contratti a favore di terze parti o applicabili ad un numero indeterminato di soggetti limita in concreto la circolazione dei dati nel cloud;

c) le BCR sono una sorta di codice di condotta interno di cui, stante la normativa vigente, possono dotarsi solo i titolari del trattamento (criticità ad es. per cloud provider inquadrati come responsabili). Tale codice di condotta per essere efficace deve venire approvato dalle autorità garanti (o comunque della Lead Authority), approvazione particolarmente difficile da ottenere. Inoltre, le BCR hanno un valore esclusivo infragruppo. Ossia i dati possono, in virtù delle BCR, circolare unicamente all'interno delle società di uno stesso gruppo (criticità con riferimento a eventuali trasferimenti a subfornitori del principale cloud provider).

d) il Safe Harbor è un meccanismo che si basa su un'autocertificazione del soggetto di diritto statunitense circa l'aderenza a questo programma (criticità con riferimento al valore reale di compliance). Inoltre, esso abilità

unicamente trasferimenti di dati da un soggetto in Europa a un soggetto negli Stati Uniti, eventuali altri trasferimenti all'interno del cloud non sarebbero dunque coperti.

Emerge da questa veloce ricognizione come occorrano nuove soluzioni per abilitare trasferimenti di dati personali in contesti extra-europei nei quali non sia garantito un livello di protezione "adeguato", assicurando una tutela concreta dei dati dei soggetti interessati. Ad oggi è dunque consigliabile per le PA esigere e richiedere garanzie che i dati non vengano trasferiti verso paesi fuori dallo SEE nei quali non sia garantito un livello di protezione 'adeguato' agli standard comunitari. Una limitazione che in alcuni casi peraltro si incrocia con quanto disposto della disciplina relativa a specifici settori, che a volte non consente nemmeno la circolazione del dato all'esterno dei confini nazionali.

VALUTAZIONE DEI RISCHI E DELLE GARANZIE

Nella valutazione dei servizi cloud computing si devono considerare le opportunità offerte da tale modello di approvvigionamento dei servizi IT rispetto all'efficacia ed efficienza dei meccanismi di gestione della sicurezza offerti dal CSP. È quindi importante che vengano ben identificati gli ambiti di valutazione, ovvero è necessario porsi preliminarmente le seguenti domande:

1. Quali specifici rischi e minacce sono connaturati nella scelta di un determinato servizio?
2. Quali garanzie devono essere fornite dal CSP ?

Pertanto si possono definire due macro ambiti in cui concentrare le valutazioni: l'ambito dei rischi e l'ambito delle garanzie.

Nell'**ambito dei rischi** il CSC deve valutare i seguenti aspetti:

- reputazione, storia e sostenibilità del CSP
- leggi applicabili e conformità legale
- allocazione di ruoli e responsabilità tra CSP and CSC
- diritto di auditing
- accesso di terze parti alle informazioni sensibili e riservate
- segregazione dei dati tra clienti (in particolare nei cloud di tipo pubblico)
- accessibilità dei dati e dei servizi (qualità del trasporto dati dell'architettura dell'infrastruttura cloud)
- portabilità dei dati e delle applicazioni
- Interoperabilità ed integrazione
- cancellazione sicura e in tempi definiti dei dati

Nell'**ambito delle garanzie** il CSC deve valutare i seguenti aspetti:

- **Trasparenza** - il CSP deve dimostrare l'esistenza di sistemi di controllo robusti ed efficaci e che le informazioni dell'utente siano ben protette da accessi non autorizzati
- ***Privacy*** - il CSP deve applicare leggi e norme sul trattamento dei dati sensibili, di gestire adeguatamente (su contratto) diritti ed obblighi in materia di notifiche di incidenti, trasferimento dati, cambi di ruoli e accessi ai dati da parte delle forze dell'ordine. Particolare attenzione sulla gestione del flusso transnazionale delle informazioni.
- **Conformità** - il CSP deve supportare l'azienda cliente ad effettuare gli audit sulla conformità a leggi e/o norme di settore che interessano i dati trasferiti nel cloud
- **Certificazioni** - il CSP dovrebbe dare evidenza di audit di terze parti o report adeguati sulla corretta esecuzione dei servizi in cloud
- **Contratto** – tra altre cose, come ad esempio la definizione di Service Level Agreements e penali per la non rispondenza, il contratto deve contemplare il caso in cui siano necessarie delle modifiche delle compliance (es.

Nuove regolamentazioni di Privacy o di settore) con modalità non punitive per il cliente e considerare anche il diritto all'Audit.

STRUMENTI DI GESTIONE DEL RISCHIO

In risposta al diffuso bisogno di fiducia nel mercato dei servizi cloud sono stati effettuati studi e sviluppati metodi per l'analisi e la gestione della sicurezza che possono essere utili per guidare le pubbliche amministrazioni nell'approvvigionamento di servizi IT di tipo cloud. La valutazione deve essere effettuata con uno o più strumenti che consentano di:

- valutare il rischio di utilizzare un determinato servizio cloud
- comparare diverse alternative cloud
- definire il proprio profilo di rischio e identificare adeguati meccanismi di protezione
- supportare la creazione di adeguati SLA e KPI
- monitorare l'esecuzione degli SLA e KPI tramite i contratti

Nel seguito si riassumono le caratteristiche di alcuni degli strumenti attualmente disponibili.

STRUMENTO 1: ENISA - INFORMATION ASSURANCE FRAMEWORK

Fornisce una sintetica suddivisione delle responsabilità fra CSC e CSP in termini di contenuti delle informazioni dei CSC, di gestione degli incidenti di sicurezza e di protezione dei dati dei CSC.

Prevede un questionario, per controlli generali, suddiviso in 10 "domini":

1. Personnel security: gestione del personale IT;
2. Supply-chain assurance: definizione di accordi con terze parti;
3. Operational security: tematiche generali sull'infrastruttura IT;
4. Identity and access management: autenticazione e autorizzazione oltre alla cifratura dei dati dei CSC;
5. Asset management: gestione dell'hardware e software da parte del CSP;
6. Data and Services Portability: valutazione del lock-in;
7. Business Continuity Management: recovery anche da disastri e gestione degli incidenti;
8. Physical security: misure di protezione dell'infrastruttura fisica IT da parte del CSP;
9. Environmental controls: gestione degli ambienti in cui risiede l'infrastruttura IT;
10. Legal requirements: eventuali obblighi di legge del CSC anche sovranazionali.

STRUMENTO 2 : ENISA - SECURITY AND RESILIENCE IN GOVERNMENTAL CLOUD

Consiste in una metodologia di 7 passi con la quale individuare la soluzione architetturale idonea per le esigenze organizzative. Il modello decisionale proposto, prevede nativamente gli aspetti di sicurezza e resilienza.

I passi della metodologia prevedono elementi da considerare per effettuare un'analisi dei requisiti sulla base dei quali selezionare l'architettura IT:

1. *Business/Operational, Legal and Regulatory;*
2. *Security and Resilience;*
3. *IT services - Architectural options and Delivery models;*
4. *Comparative Risk Assessment (SWOT or Risk Analysis & Assessment);*
5. *Identify Threats, Weaknesses;*
6. *Prepare Request for Proposal (RfP);*
7. *Risk Treatment.*

STRUMENTO 3 : CSA - CONSENSUS ASSESSMENTS INITIATIVE (CAI)

Consiste in un elenco di domande, basate su documenti CSA Guidance e CSA Cloud Control Matrix (versione 1.1) suddivise in 11 "domini":

- *Compliance*: controllo (audit, assessment) interno all'organizzazione e rispetto della proprietà intellettuale;
- *Data Governance*: gestione e protezione dei dati;
- *Facility Security*: politiche per la sicurezza degli ambienti interessati dai processi cloud;
- *Human Resources Security*: gestione del personale a partire dalla selezione;
- *Information Security*: controlli relativi agli aspetti della security per il CSC;
- *Legal*: accordi con terze parti;
- *Operations Management*: gestione della documentazione di sistemi, processi o procedure;
- *Risk Management*: processi per la gestione del rischio;
- *Release Management*: processi per la messa in esercizio di nuovi software;
- *Resiliency*: processi per la business continuity;
- *Security Architecture*: controlli relativi agli aspetti di sicurezza per il CSP.

Strumento 4 : CSA - Cloud Control Matrix

Matrice che individua i principali controlli da effettuare e su cui si basano le domande della CS CAI. Per ogni area individuata è riportata un'associazione con i principali standard di riferimento.

La CCM è attualmente alla versione 1.2 che, rispetto a quella della CAI, introduce il "dominio":

- *Human Resources*: gestione della cessazione dei contratti con il personale.

Strumento 5 : CAMM - Common Assurance Maturity Model

Consiste in un framework le cui caratteristiche prevedono oggettività, consistenza e completezza, il cui scopo è quello di garantire la gestione del rischio in maniera trasparente in tutto il processo produttivo.

I principali benefici dovuti alla sua adozione sono:

- valutazione e comparazione oggettiva dei CSP;
- riduzione di costi e tempi;
- prevenzione di situazioni di lock-in rendendo più snelli i modelli di business;
- conformità con la maggior parte degli standard;
- gestione del rischio incentrato sulla disponibilità, confidenzialità ed integrità delle informazioni.

Strumento 6 : Proposed Security Assessment and Authorization for U.S. Government Cloud Computing

Matrice che individua i principale controlli da effettuare in conformità con le linee guida del NIST. Per ogni area individuata sono generalmente riportati due tipi di controlli: uno a basso impatto ed uno a medio. Le aree individuate sono:

1. *Access Control*: procedure e politiche per l'accesso ai sistemi indistinto per CSP e CSC;
2. *Awareness and Training*: politiche di sensibilizzazione alle sicurezza;
3. *Audit and Accountability*: tracciamento degli accessi e delle attività;
4. *Assessment and Authorization*: processo per migliorare il livello di sicurezza;
5. *Configuration Management*: gestione della configurazione dei sistemi;
6. *Contingency Planning*: processo di business continuity;
7. *Identification and Authentication*: autenticazione ed autorizzazione anche di dispositivi;
8. *Incident Response*: gestione degli incidenti;
9. *Maintenance*: manutenzione dei sistemi e del personale associato;
10. *Media Protection*: politiche di gestione, mantenimento e trasporto dei dati;

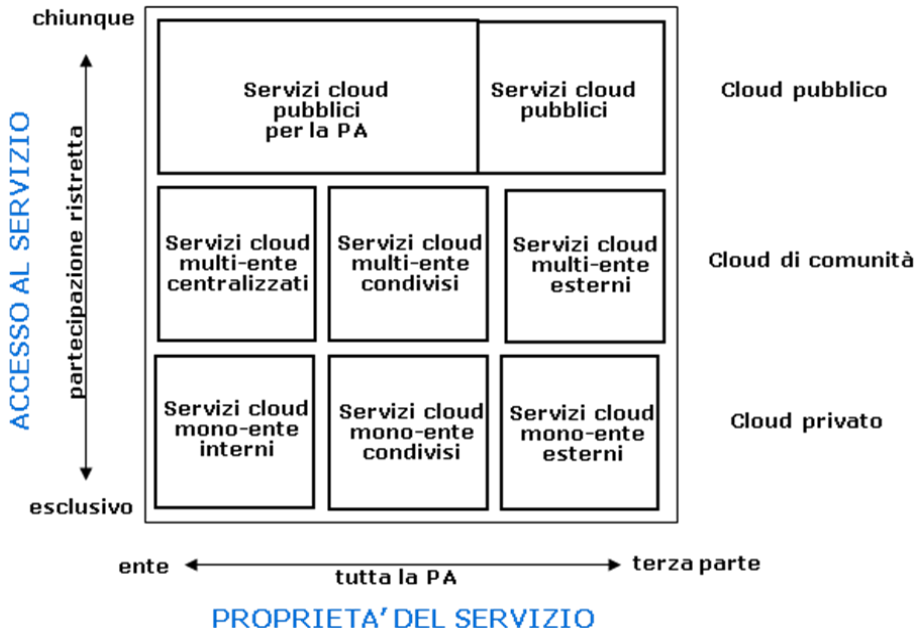
11. *Physical and Environment Protection*: politiche per la gestione degli accessi e protezione da disastri naturali;
12. *Planning*: pianificazione generale della sicurezza con attenzione alla privacy;
13. *Personnel Security*: gestione del personale, anche di terze parti, con attenzione alla cessazione delle prestazioni;
14. *Risk Assessment*: processi di verifica delle vulnerabilità e gestione;
15. *System and Services Acquisition*: gestione del ciclo di vita del software;
16. *System and Communication Protection*: controlli relativi alla sicurezza IT del CSC relativamente al "data at motion";
17. *System and Information Integrity*: controlli relativi alla sicurezza IT del CSC relativamente al "data at rest".

3.4 INFRASTRUTTURE TECNOLOGICHE

Nel definire un approccio pragmatico per l'adozione del modello cloud da parte delle PA, considerando gli investimenti già fatti per il consolidamento e la virtualizzazione dei proprio data center, possiamo identificare i seguenti percorsi:

- grandi enti che si propongono in qualità di cloud provider per sé stessi e per altre PA;
- piccoli enti che si configurano esclusivamente come cloud consumer, acquistando servizi dai cloud provider.

In realtà, questi due scenari appartengono ad una complessa tassonomia dei servizi cloud all'interno della pubblica amministrazioni riassunta nella figura seguente, ricavata da [GART10]. Nella figura, i diversi modelli organizzativi del cloud nella pubblica amministrazione sono classificati secondo le due dimensioni della proprietà del servizio e dell'accesso al servizio.



Tassonomia del cloud nella pubblica amministrazione (adattato da: Gartner)

Dal punto di vista delle PA che si propongono come fornitori di servizi cloud, il percorso di adozione dovrà preliminarmente prevedere il completamento dei processi di consolidamento e di virtualizzazione delle proprie infrastrutture, estendendola anche alle applicazioni critiche. Ciò consentirà di ottenere il massimo valore aggiunto dalla condivisione delle risorse, introducendo i vantaggi di scalabilità e flessibilità propri di un cloud provider. Successivamente potranno essere introdotti gli ulteriori livelli di automazione e governance richiesti in un cloud.

D'altro canto l'adozione del cloud come modello di fruizione dell'IT ha un notevole impatto sia sulle modalità operative di conduzione di un data center (*governance*) sia sulle infrastrutture IT (sistemi, network e storage area network).

LA PA COME EROGATORE DI SERVIZI CLOUD (CLOUD PROVIDER)

Questo primo scenario è rivolto principalmente alle grandi organizzazioni della PA, dotate di data center rilevanti e già fortemente orientati alla virtualizzazione e al consolidamento che, al fine di razionalizzare le risorse IT, decidono di adottare il modello cloud per l'erogazione di servizi ai propri dipartimenti, ad altre amministrazioni e organizzazioni o ai cittadini.

Gli scenari di adozione del cloud da parte delle PA, in qualità di fornitori di servizi, possono essere diversi e anche tra loro complementari. La corretta adozione del modello richiede, comunque, che vengano soddisfatti una serie di requisiti alla base delle infrastrutture che supportano il cloud.

INTEGRAZIONE E IMPATTI CON L'INFRASTRUTTURA ESISTENTE

Viste le caratteristiche specifiche della PA, il modello di cloud privato o di community può essere considerato prevalente. È infatti difficile immaginare lo scenario in cui tutti i servizi, le banche dati, le capacità gestionali dell'Amministrazione siano trasferite ad un provider pubblico.

Se l'Amministrazione decide di mantenere alcune applicazioni presso il proprio datacenter è necessario che le interfacce applicative utilizzate siano standard (ad es. SOAP o REST) e sia supportata l'integrazione dei dati tra le piattaforme interne e del Service Provider.

Se l'Amministrazione decide di mantenere alcune basi dati, deve essere posta la massima attenzione ai problemi di latenza e quindi ai tempi di risposta dell'applicazione derivanti dall'interazione tra le piattaforme, che comunque deve essere supportata.

Se l'Amministrazione decide di mantenere la gestione della sicurezza e del monitoraggio del sistema, è necessario scegliere soluzioni in cloud che lo permettano, per esempio nel caso di adeguamento della propria infrastruttura con risorse cloud di tipo IaaS.

Se l'Amministrazione decide di mantenere la massima flessibilità, volendo spostare le macchine virtuali dal proprio cloud ad un altro e viceversa, è necessario verificare l'utilizzo di strumenti di interazione e gestione standard sia internamente che sulle piattaforme del Provider.

LA PA COME FRUITORE DI SERVIZI CLOUD (CLOUD CONSUMER)

La realizzazione e l'adeguamento dell'infrastruttura informatica è una delle principali difficoltà che le piccole e medie Amministrazioni devono affrontare a causa dei lunghi e complessi processi legati all'acquisizione delle componenti infrastrutturali oltre che ai tempi di realizzazione.

Le soluzioni di cloud computing, oltre ad evitare la realizzazione e la gestione in casa delle infrastrutture IT, riducono drasticamente i tempi di acquisizione delle tecnologie in quanto il processo si sostanzia con la sottoscrizione di un contratto con il service provider.

L'adozione di servizi in cloud favorisce dunque il recupero della prontezza di risposta della pubblica amministrazione alla crescente domanda di servizi agevolando il mantenimento delle infrastrutture allo stato dell'arte.

Adottando questo modello è possibile:

- migrare da un modello di erogazione dei servizi con infrastrutture IT *in house* dedicate, che prevede tempi lunghi e ingenti investimenti per la progettazione, la selezione delle tecnologie, l'installazione e la gestione di data center, ad un modello che prevede l'acquisizione delle migliori tecnologie *as a service*, a costi sostenibili grazie alle economie di scala del service provider;
- adeguare velocemente l'infrastruttura IT a seguito della variazione dei carichi di lavoro;
- eliminare molte delle attività e degli investimenti necessari a pianificare e gestire l'upgrade delle tecnologie acquisite al fine di contrastare l'obsolescenza dell'infrastruttura.

Inoltre il cloud, basando il suo modello sull'utilizzo di risorse condivise e facilmente accessibili in modalità on-demand, permette un recupero dell'efficienza attraverso:

- l'incremento dell'utilizzo delle risorse IT (dall'attuale valore medio del 30% ad un valore stimato di circa il 60-70%);
- l'eliminazione dei sistemi duplicati e ridondanti;
- l'aumento della produttività nello sviluppo applicativo e nella gestione delle applicazioni e degli utenti finali del servizio.

Nell'acquisizione di servizi cloud da parte delle Amministrazioni bisogna comunque valutare che le infrastrutture ed i servizi richiesti abbiano le caratteristiche per essere utilizzati in cloud e che l'offerta del cloud provider rispetti tutte le caratteristiche necessarie per una fruizione affidabile e sicura.

Nel prosieguo si evidenziano i principali scenari che vedono la PA come *cloud consumer* e si indicano i percorsi decisionali per la scelta del fornitore ed i principali punti di attenzione da considerare nella fruizione di servizi cloud (IaaS, PaaS, SaaS).

La disponibilità di servizi informatici in modalità cloud apre alla PA diversi scenari di fruizione che si possono riassumere nei modelli di seguito elencati.

- **Utilizzo di servizi cloud ospitati su una infrastruttura cloud interna (on site private cloud), oppure infrastruttura cloud interna gestita da remoto da un outsourcer (private managed)**

  Questo modello prevede la fruizione di servizi tipicamente erogati nell'ambito di una stessa organizzazione (es. un ministero verso i propri dipartimenti). L'infrastruttura cloud interna potrebbe essere gestita da un outsourcer esterno per sgravare l'amministrazione dalle attività di gestione e dalla necessità di avere specifici skill. In generale questa modalità permette il completo controllo da parte dell'amministrazione erogante sull'infrastruttura, sugli aspetti di sicurezza e sui dati.

- **Utilizzo di servizi cloud su una infrastruttura cloud dedicata ospitata da un outsourcer (outsourced private)**

  Questo modello prevede un cloud privato costituito su una infrastruttura ospitata in un data center esterno. È il caso di una amministrazione che vuole creare il suo cloud privato per l'erogazione di servizi all'interno della sua organizzazione, ma non vuole mettersi in casa infrastrutture e pertanto si affida ad un provider esterno che provvede a realizzare l'infrastruttura cloud privata. L'amministrazione pagherà per il servizio cloud sostenendo maggiori costi derivanti da una infrastruttura a lei dedicata.

  Rispetto al modello precedente, nella fruizione di servizi da questa tipologia di cloud, maggiore attenzione deve essere posta su come le infrastrutture dei diversi clienti vengono mantenute separate in casa del cloud provider e sui meccanismi di sicurezza adottati per l'accesso ai servizi dall'esterno.

- **Utilizzo di servizi cloud nell'ambito di una comunità formata da diversi soggetti PA (*on site community cloud*) eventualmente su una infrastruttura in outsourcing (*outsourced community cloud*)**

  Il cloud di comunità è formato da un insieme di cloud delle singole amministrazioni che decidono di aggregarsi per fornirsi reciprocamente i servizi ottimizzando quindi complessivamente gli investimenti da effettuare. In questa tipologia di cloud ognuna delle amministrazioni partecipanti può fungere da erogatore, da fruitore oppure contemporaneamente da erogatore e fruitore dei sevizi. In genere i servizi sono progettati sulle specifiche esigenze dei fruitori che costituiscono la comunità rispettando gli standard e le normative di sicurezza richieste.

  Nell'usufruire servizi da un community cloud particolare attenzione va posta alla sicurezza degli accessi ai singoli perimetri delle diverse amministrazioni della community.

  Questo modello è efficiente se le esigenze delle singole amministrazioni risultano simili o complementari tra loro.

- **Utilizzo di servizi cloud da un provider esterno pubblico (*public cloud*)**

Il modello *public* prevede l'acquisizione di servizi offerti da cloud provider esterni attraverso internet. I fornitori erogano i servizi dai propri data center con infrastrutture che sono condivise tra i clienti. Il fruitore in questo modello non ha nessun controllo sulla piattaforma, sui dati, sui meccanismi di gestione dei tenant, sulla sicurezza, sull'aderenza agli standard di portabilità ed interoperabilità. Anche la collocazione geografica dei dati è a discrezione del fornitore che potrebbe allocarli nelle differenti sedi geografiche, anche internazionali, dei propri data center. Solo l'attenta verifica di come il provider soddisfa queste caratteristiche, anche in funzione del servizio cloud da acquisire, permetterà l'utilizzo di questo modello.

Rispetto agli altri modelli, in questo caso è necessario porre la massima attenzione alle normative vigenti riguardo il trattamento dei dati.

- **Utilizzo di servizi cloud erogati in differenti modalità: private, community o public (Hybrid cloud)**

Il modello ibrido prevede che un'Amministrazione utilizzi contemporaneamente più modelli di cloud (anche integrati nella propria infrastruttura). Per esempio potrebbe utilizzare un cloud pubblico per fruire di servizi non core che non richiedono particolari requisiti di sicurezza e contemporaneamente un cloud privato per i servizi legati a dati sensibili che devono rimanere all'interno dell'Amministrazione. Altro esempio di impiego è l'utilizzo del proprio cloud privato come modello primario che in momenti di maggior picco di lavoro possa essere integrato con risorse acquisibili da un cloud pubblico. Il cloud ibrido può essere molto complesso soprattutto se i servizi acquisiti con i diversi modelli cloud devono interoperare ed essere integrati.

Nel caso del cloud ibrido una valutazione attenta delle caratteristiche va fatta caso per caso applicando i criteri di valutazione dei singoli modelli e valutando la complessità dell'integrazione.

4. SINTESI DELLE RACCOMANDAZIONI E PROPOSTE PER UN'AGENDA CONDIVISA

In questo capitolo quanto discusso nei capitoli precedenti viene riassunto sotto forma di raccomandazioni e proposte sintetiche raggruppate negli stessi ambiti utilizzati nel resto del documento.

4.1 INDICAZIONI DI CARATTERE GENERALE

Condividere le regole e i cammini di adozione dei servizi cloud

La condivisione a livello nazionale di regole comuni nell'adozione dei servizi cloud appare un'esigenza largamente condivisibile, peraltro in sintonia con l'art. 117 della Costituzione [COST]. Anche a livello internazionale, le strategie di eGovernment adottate da alcuni Paesi (cfr. ad esempio [UKICT] e [VIV10]) suggeriscono la necessità di elaborare una politica nazionale che comprenda i temi affrontati in queste Raccomandazioni, in particolare la sicurezza e la privacy, l'interoperabilità, gli aspetti economici, legali e contrattuali e l'identificazione delle tipologie di servizi di *front end* o di *back office* che meglio si prestano ad una migrazione sul cloud.

Diversi strumenti per la *governance* del processo di adozione del cloud da parte delle pubbliche amministrazioni possono essere ipotizzati, tra i quali:

- un comitato *ad hoc* coordinato o sostenuto da DigitPA al quale partecipino prevalentemente rappresentanti delle pubbliche amministrazioni impegnate in progetti di adozione di servizi cloud;
- un tavolo permanente che riunisca i diversi *stakeholder* interessati nell'adozione di servizi cloud, eventualmente come evoluzione del gruppo di lavoro che ha fornito supporto all'elaborazione di queste Raccomandazioni;
- altri strumenti preesistenti di *governance* nel campo dell'amministrazione digitale.

Accelerare e approfondire la razionalizzazione dei grandi data center pubblici

Sia pure con finalità e modalità diverse, molte grandi organizzazioni stanno accompagnando all'adozione dei servizi cloud un processo di evoluzione e migrazione delle infrastrutture ICT *legacy*. L'esempio forse più citato è ancora quello degli USA, che hanno avviato in parallelo la *Federal Data Center Consolidation Initiative* e la *Federal Cloud Computing Initiative* [CIOUS]. Dal lavoro di fondazione compiuto dal NIST (*National Institute of Standards and Technology*) fino alla creazione del portale Apps.Gov, queste due iniziative rappresentano importanti punti di riferimento anche per altre realtà nazionali.

Nel nostro Paese, un esempio notevole, ma certo non l'unico, di questa sinergia è rappresentato dal nuovo data center di ENI, che garantirà l'altissima affidabilità richiesta dalle esigenze informatiche aziendali insieme ad un'efficienza energetica di eccellenza. La realizzazione del data center è accompagnato dal consolidamento degli applicativi con un risparmio dell'ordine delle decine di milioni di euro [ENIGDC].

L'utilizzo del cloud da parte della pubblica amministrazione sarebbe fortemente favorito da un intervento immediato di razionalizzazione dei data center e di introduzione nelle piattaforme applicative di elementi di modularità e di standardizzazione. Questo intervento, peraltro, rappresenta già di per sé un'occasione per conseguire una decisa riduzione del patrimonio applicativo, una forte accelerazione del suo riuso, una distribuzione delle maggiori basi di dati fondata sulla razionalizzazione degli accessi e delle prestazioni anziché sulle politiche, finora prevalenti, basate sulla

duplicazione[2] e sulla ridondanza. La logica di progressione appena esposta consente di scegliere in modo mirato gli oggetti da far emigrare nei diversi tipi di cloud offerti dal mercato.

Valutare costi e benefici dei cloud privati e di comunità per la pubblica amministrazione

Sebbene l'adozione dei servizi cloud si giustifichi prima di tutto per i risparmi diretti legati alle economie di scala caratteristiche dei grandi cloud di tipo pubblico globali, molti fattori possono opporsi alla loro adozione generalizzata, sia nel settore privato che in quello pubblico. Gartner [GART11] prevede ad esempio che, nonostante l'attuale tasso annuo di crescita della spesa per servizi cloud di tipo pubblico del 19%, entro il 2015 questi servizi rappresenteranno meno del 5% della spesa IT complessiva.

Altre forme di cloud, di tipo privato o di comunità, vengono spesso considerate come un'alternativa a quelli di tipo pubblico in vista di un maggiore controllo, del rispetto di vincoli organizzativi o territoriali e di vantaggi economici indiretti derivanti da razionalizzazione, accorpamento e riuso delle risorse informatiche esistenti. La realizzazione di *cloud data center* di tipo privato o di comunità deve però essere attentamente giustificata in quanto i vantaggi economici diretti potrebbero ridursi a causa delle minori economie di scala o di barriere digitali conseguenti ad una regolazione incompleta o non tempestiva.

La valutazione delle soluzioni e delle architetture dovrà anche tenere conto dei diversi ruoli a livello architetturale [NISTCCRA11] e in particolare dei ruoli di fornitore e di *broker* di servizi cloud oppure di fruitore degli stessi servizi. È evidente che diverse amministrazioni, enti e loro società strumentali potranno ricoprire in modo naturale l'uno o l'altro dei ruoli. La tassonomia di configurazioni proposta da Gartner [GART10] sulla base di caratteristiche quali la proprietà dei servizi o l'accesso ai servizi conferma la molteplicità di valutazioni necessarie anche in ambito *government*.

Promuovere la disseminazione e lo scambio di esperienze nelle pubbliche amministrazioni

I documenti prodotti dal gruppo di lavoro "Cloud computing e pubblica amministrazione", che hanno formato la base di queste Raccomandazioni, mostrano che l'offerta e la natura stessa dei servizi cloud sono in piena evoluzione e lo resteranno nel prevedibile futuro. È perciò consigliabile estendere e rendere sistematica la diffusione di informazioni e di buone pratiche all'interno del settore pubblico attraverso gli strumenti più efficaci disponibili. Tra questi, si ipotizza in particolare l'istituzione di una comunità che raccolga gli esperti di cloud nelle pubbliche amministrazioni.

Come già segnalato in altri punti, diverse modalità di svolgimento di questa importante funzione sono possibili. Con la dovuta attenzione alle peculiarità nazionali, alcune esperienze di altri Paesi, come i *Chief Information Officers Councils* in USA e UK [CIO], possono offrire ispirazione e indicare criticità. DigitPA ritiene di potere contribuire a svolgere questa funzione.

Promuovere la ricerca e la sperimentazione sul Government cloud

Government Cloud (o gCloud) è un'espressione utilizzata per indicare le specifiche politiche tecnologiche per promuovere l'adozione dei servizi cloud nella pubblica amministrazione. Queste possono comprendere ad esempio la creazione di cloud di tipo privato riservati alla pubblica amministrazione e ai suoi utenti, oppure il consolidamento dei data center e delle applicazioni in uso dalla pubblica amministrazione, oppure il ricorso alle modalità innovative di erogazione dei servizio di eGovernment rese possibili dal paradigma cloud.

Un maggiore sostegno alla ricerca sul cloud viene invocato già da alcuni anni a livello europeo (cfr. ad esempio [DGI10]). Mentre la partecipazione nazionale a questi sforzi è certamente opportuna, un contributo mirato alla ricerca e alla

[2] Uno degli strumenti per evitare la duplicazione è il riuso dei programmi informatici cui è dedicato, l'art. 69 di [CAD05] dove sono indicate modalità concrete per garantire il riuso dei programmi e dei singoli moduli sviluppati per conto e a spese delle pubbliche amministrazioni.

sperimentazione di soluzioni G-Cloud a livello nazionale potrebbe contribuire ad un'adozione sistemica del cloud da parte della pubblica amministrazioni italiana, con possibili importanti ricadute sia in termini di spesa pubblica che di efficienza energetica.

Curare da vicino gli aspetti internazionali

Come già sottolineato, nonostante le realizzazioni concrete possano variare in base ai diversi contesti, l'adozione di servizi cloud si giustifica generalmente per un uso su scala relativamente grande. Anche in ambiti più limitati, come ad esempio quello nazionale o europeo, risulta difficile immaginare politiche di adozione del cloud che non seguano da vicino l'evoluzione degli standard, la disponibilità dei finanziamenti, l'offerta dei fornitori e le stesse esperienze sviluppate al di fuori dei confini nazionali.

L'Unione europea ha da tempo avviato azioni importanti, anche economicamente, per promuovere l'uso del cloud da parte degli Stati membri (cfr. ad esempio i programmi CIP – ICT PSP [CIP11] e ISA [ISA11]). A breve termine verrà annunciata una strategia cloud europea che indicherà prevedibilmente nuove iniziative e renderà disponibili nuovi finanziamenti mirati che sarà certamente opportuno coordinare con le iniziative nazionali in questo campo.

Più in generale, appare indispensabile curare, nei casi via via rilevanti, i rapporti con tutti gli *stakeholder* internazionali che operano per l'evoluzione dell'assetto normativo e degli standard o promuovono iniziative di studio e progettuali in questo campo.

Avviare progetti-pilota in settori prioritari

I servizi cloud rappresentano un'opportunità per progettare e rendere disponibili a costi marginali servizi digitali di ogni tipo. Alcuni casi di uso presentano però caratteristiche che li rendono particolarmente adatti alla realizzazione, in tempi brevi e con elevati ritorni, di progetti-pilota o di sistemi direttamente operativi. Tali caratteristiche comprendono un'ampia base di utenti, connettività adeguata, copertura dell'intero territorio nazionale, presenza di esperienze che permettano subito una graduale digitalizzazione di onerosi processi di tipo tradizionale.

Molte sono le prospettive di applicazione del paradigma *cloud* per la raccolta, gestione e diffusione dei dati prodotti dal mondo della **scuola**. Procedure automatizzate di scrutinio o di verbalizzazione degli esami, a volte ispirate a modalità cloud, sono già utilizzate in molte scuole e università italiane. Molti altri processi generati dall'interazione tra studenti, famiglie, insegnanti e amministrazione (e che quindi coinvolgono la stragrande maggioranza dei cittadini) possono essere trasformati in servizi cloud in tempi brevi. Strumenti di eLearning basati sul cloud e accessibili da dispositivi mobili sono ormai ampiamente diffusi a livello globale.

Tutte le **amministrazioni di piccole e medie dimensione** devono ottemperare a requisiti di legge che possono implicare impegni economici ed organizzativi gravosi o anche irrealistici. Ad esempio, l'articolo 50-bis ("Continuità operativa") del Codice dell'amministrazione digitale [CAD05] delinea gli obblighi, gli adempimenti e i compiti che spettano alle pubbliche amministrazioni, a DigitPA e ai ministri delegati per la Funzione pubblica e per l'Innovazione tecnologica ai fini dell'attuazione della continuità operativa. In particolare ogni amministrazione deve predisporre il piano di continuità operative ed il piano di *disaster recovery* che saranno adottati da ciascuna sulla base di appositi studi di fattibilità tecnica, sui quali è obbligatoriamente acquisito il parere di DigitPA [DIG11]. Se l'amministrazione ha acquisito dei servizi cloud ed ha parte dei suoi dati su un cloud esterno, dovrà considerare anche questo scenario nelle soluzioni tecniche per la salvaguardia dei dati e delle applicazioni informatiche.

Anche la **sanità** presenta le caratteristiche sopra richiamate, nonostante la delicatezza dei dati trattati e l'affidabilità richiesta alle applicazioni. Alcune esperienze pilota in Italia, tra le quali quella della ULSS 8 di Asolo (TV), hanno realizzato la digitalizzazione di un ampio ventaglio di servizi digitali di back-office e di front-office che spaziano dalla ricetta elettronica fino alla scheda sanitaria individuale, alla prenotazione degli esami, al pagamento elettronico dei

ticket e al ritiro dei referti. Anche da questa esperienza è scaturito un documento di raccomandazioni sul cloud computing in sanità (cfr. [ULS11]).

4.2 Aspetti economici e giuridici

Cogliere le opportunità sistemiche per la pubblica amministrazione e per il paese

Da quanto è possibile comprendere in un quadro in rapida evoluzione, l'adozione dei servizi cloud, per loro natura basati su ottimizzazioni di carattere generale e su larghissima scala, sarà in grado di produrre risparmi economici diretti in tutti i settori economici.

A livello macroeconomico, numerosi e autorevoli studi indicano i possibili benefici economici, anche in termini di aumento del PIL, che l'adozione del modello cloud può portare a livello nazionale e regionale (cfr. ad esempio [ETR09], [ARP11]).

Per le grandi organizzazioni, compresa evidentemente la pubblica amministrazione, è possibile intravedere anche ulteriori vantaggi indiretti derivanti, ad esempio, dalla forte spinta verso la razionalizzazione delle infrastrutture ICT e degli asset informativi che il ricorso al cloud presuppone.

Valutare tutti i costi della migrazione al cloud

A livello di singola pubblica amministrazione, è possibile valutare l'impatto che l'adozione di soluzioni cloud comporta attraverso modelli quantitativi (cfr. ad esempio [AVE11], [VMW11], [MSI11]) che descrivono analiticamente costi e benefici delle diverse soluzioni e consentono un confronto delle diverse alternative di investimento in base all'analisi del TCO (*Total Cost of Ownership*), dell'IRR (*Internal Rate of Return*) e del ROI (*Return on Investment*).

L'orizzonte temporale da considerare, qualunque sia il modello adottato, dovrà essere di medio-lungo periodo per evitare il rischio di un'analisi influenzata dai costi di migrazione previsti nelle fasi iniziali di un progetto di cloud computing, costi che sono invece assenti nei progetti che mantengono invariati i processi, le applicazioni e le tecnologie. Le diverse soluzioni dovrebbero essere comparate sulla base di tutte le tipologie di costi stimabili (in conto capitale, operativi, di opportunità).

Raccomandazioni dettagliate relative ai percorsi di adozione sono già disponibili (cfr. ad esempio [NISTCON11]). In sintesi, si raccomanda di prevedere almeno le seguente azioni:

- Condurre un *assessment* del proprio sistema informativo (processi, applicazioni, infrastrutture) attraverso società indipendenti
- Analizzare la mappa dei processi, delle applicazioni, degli ambienti elaborativi, dei costi relativi di conduzione e manutenzione per individuare le parti candidate al cambiamento;
- Scegliere un modello quantitativo per la valutazione delle alternative di investimento;
- Utilizzare metriche e *benchmark* condivisi per la misura delle caratteristiche dei sistemi hardware, software, dei servizi e per il confronto dei costi associati alle diverse componenti
- Svolgere le prime esperienze cloud su applicazioni non *mission critical*

Adottare alcuni accorgimenti per superare l'incompletezza del quadro normativo

In via generale, il contratto di fornitura di servizi cloud sembra rientrare nella categoria dell'appalto di servizi disciplinato dall'art. 1655 del Codice civile [BEL11]. Tuttavia non esistono disposizioni nazionali o comunitarie specifiche che disciplinino i contratti relativi a servizi cloud. Gli strumenti contrattuali attualmente in uso appartengono alla categoria di contratti "per adesione", sostanzialmente non negoziabili e talvolta non coerenti con le disposizioni sugli

appalti pubblici. Risulta perciò opportuno richiamare le previsioni del D. Lgs. 39/1993, del D. Lgs. 163/2006, del D. Lgs. 177/2009 e del D.P.R. 207/2010.

In termini generali, a causa della prevalenza degli aspetti tecnologici, l'aggiudicazione dovrebbe essere a favore dell'offerta economicamente più vantaggiosa e la determinazione dell'importo a base di gara dovrà basarsi su una completa analisi dei costi della soluzione cloud. Nei casi previsti, per gli aspetti innovativi dei servizi cloud, la richiesta del parere di congruità da parte di DigitPA dovrebbe sempre essere accompagnata da uno studio di fattibilità [CNI06].

I diversi requisiti possono essere utilmente raggruppati in un documento - *Cloud Service Level Agreement* - che definisca e specifichi, tra l'altro, le parti contrattuali, l'oggetto della fornitura, i livelli di servizio (SLA), i trattamenti effettuati sui dati personali e la conformità alla normativa privacy applicabile (*Privacy Level Agreement* - PLA), la portabilità e interoperabilità dei servizi erogati, le eventuali penali e le verifiche di conformità.

4.3 Privacy e sicurezza

Seguire le linee-guida europee e nazionali e contribuire al loro sviluppo

In termini generali, le pubbliche amministrazioni dovrebbero avvicinarsi ai servizi cloud con un atteggiamento di consapevole prudenza, come suggerito da autorevoli istituzioni pubbliche ed indipendenti quali il Garante per la protezione dei dati personali [GAR10] ed ENISA [ENISASR11, CAT09]. Vanno perciò riprese le raccomandazioni di effettuare un'attenta valutazione dei rischi legati alla fruizione di servizi cloud al fine di preservare la riservatezza e l'integrità dei dati dei cittadini, l'integrità e la continuità dei servizi offerti, il diritto alla *privacy* e più in generale l'interesse e la sicurezza nazionale.

In particolare, tra le raccomandazioni espresse da ENISA ed attualmente in uso dal governo federale americano [NISTDOC], citiamo le seguenti:

- Creazione di un catalogo dei servizi cloud idonei per la PA
- Identificazione dei requisiti di sicurezza, protezione dei dati personali e resilienza del servizio
- Identificazione della catena di responsabilità
- Monitoraggio del rispetto dei requisiti attraverso SLA che comprendano, oltre a quelli prestazionali, parametri di sicurezza e di adattabilità ("resilienza")
- Definizione di una politica chiara circa il trasferimento dei dati all'estero
- Gestione del rischio e *audit*
- Adozione di strumenti di *auditing*
- *Incident reporting*

Contrattualizzare il rispetto della tutela dei dati personali

Si riscontra un'obiettiva difficoltà di applicare al cloud i tradizionali schemi della vigente normativa in materia di tutela dei dati personali. Ad esempio, non è scontato che il cloud provider sia da ritenersi correttamente un Responsabile esterno del trattamento. Questo fatto, abbinato alla varietà dei dati trattati (dati 'comuni', sensibili, giudiziari ecc.), agli ambiti di trattamento ed alle caratteristiche dei servizi cloud, fa sì che la migrazione di dati personali nel cloud da parte della pubblica amministrazione non possa essere affrontata in senso astratto o generico, ma vada attentamente analizzata e calibrata sulle esigenza e le caratteristiche dello specifico trattamento. È quindi preventivamente necessario individuare, caso per caso, quali tipologie di dati e di trattamenti si intenda migrare, definire i relativi obblighi e responsabilità in capo alla pubblica amministrazione ed al cloud provider e verificare che siano chiaramente riflessi nel contratto di fornitura cloud.

Si raccomanda in particolare di ricorrere a specifici *Privacy Level Agreement* (PLA) che definiscano i livelli e le garanzie relative alla tutela e alla sicurezza dei dati personale da parte del fornitore di servizi cloud. I PLA potrebbero riguardare

ad esempio modalità di cifratura dei dati e di controllo da parte dell'amministrazione, limitazioni al trasferimento dei dati, tracciabilità delle azioni sui dati e delle relative responsabilità, garanzie di portabilità e politiche di persistenza e di conservazione dei dati.

È anche auspicabile l'elaborazione di linee-guida specifiche per i diversi settori amministrativi, comprese indicazioni concrete e non formali, sia a livello europeo che nazionale, sugli obblighi e le responsabilità delle parti coinvolte, che contribuirebbero alla maturazione del mercato dei servizi cloud. Considerata la caratteristica architettura distribuita del cloud, sono altresì auspicabili soluzioni normative innovative che abilitino i trasferimenti in contesti extra-europei assicurando la tutela dei dati. Visti i limiti della normativa attuale, appare opportuno richiedere garanzie che i dati non vengano trasferiti all'esterno dello Spazio Economico Europeo (SEE). In questo ambito DigitPA ritiene di poter offrire utili contributi in collaborazione con il Garante per la protezione dei dati personali, anche alla luce della passata esperienza.

Definire le garanzie che devono essere fornite dai fornitori di servizi cloud

Sebbene molti dei rischi legati all'uso del cloud siano propri di qualsiasi servizio IT, alcuni di essi sono certamente caratteristici di questo paradigma. Il cloud sollecita nuove modalità di controllo e di governo nella gestione delle informazioni, nella produzione, erogazione e fruizione dei servizi IT e nella gestione dei rischi. In sintesi, il nuovo modello di *security governance* è basato sul controllo indiretto e sulla delega delle funzioni tecniche. I requisiti di sicurezza e di resilienza del servizio, la *compliance* e la protezione dei dati vengono stabiliti su base contrattuale, con la definizione di specifici *Service Level Agreement (SLA)* e *Privacy Level Agreement (PLA)*. Il raggiungimento e mantenimento dei livelli di servizio è poi regolarmente monitorato.

Una delle maggiori barriere d'ingresso al mercato dei servizi cloud da parte sia della PA che delle PMI è rappresentato dalla mancanza di trasparenza sulle pratiche di sicurezza adottate dai fornitori di servizi cloud. Al fine di ridurre questa criticità si raccomanda:

1. l'utilizzo di *framework* standardizzati per la valutazione dei fornitori, come [ENISAIAF98], [ENISASR11], [CSACCM11] e [CSACAI11]. Si tratta di liste di controllo suddivise in domini che hanno l'obiettivo di comprendere se e come un fornitore possa soddisfare i requisiti di un utilizzatore di servizi cloud;

2. l'adozione di tecnologie che consentano il monitoraggio continuo del rispetto dei requisiti dell'utente e dei termini contrattuali;

3. l'introduzione di un processo di certificazione di servizi e fornitori basato sui punti precedenti, come ad esempio il processo FedRamp proposto dal Governo Federale USA.

Valutare non solo i rischi ma anche i benefici derivanti dal ricorso al cloud

Posta la necessità di rivedere l'approccio alle gestione della sicurezza dei servizi e delle informazioni sulla base del modello di *governance* imposto dal paradigma cloud [CSA10], è opportuno sfruttare al meglio anche i vantaggi offerti in termini di sicurezza e di resilienza. Rispetto alle soluzioni che possono essere sviluppate dai fruitori di servizi cloud con i mezzi a loro disposizione, i fornitori di servizi cloud possono essere in grado di offrire soluzioni di sicurezza assai più efficaci ed efficienti grazie, tra l'altro, ai fattori di scala.

Per motivi analoghi, il modello cloud può anche contribuire a migliorare la sicurezza dei dati e dei servizi IT offerti ed utilizzati dalla PA, sia per quanto riguarda la riservatezza dei dati che la disponibilità e la scalabilità dei servizi. Questo ultimo aspetto riveste un ruolo cruciale per quei servizi al cittadino che richiedono una disponibilità pressoché continua, come ad esempio i servizi sanitari. Infine, il paradigma cloud dovrebbe essere considerato come un'opportunità per ricondurre sul piano sostanziale anziché formale l'attuazione delle leggi sulla privacy nell'IT.

4.4 INFRASTRUTTURE TECNOLOGICHE

Facilitare la sostituzione di infrastrutture IT tradizionali con servizi cloud

A causa dei complessi processi legati all'acquisizione delle componenti infrastrutturali e dei relativi tempi di realizzazione e di integrazione, il mantenimento di una infrastruttura informatica adeguata e aggiornata rappresenta una delle principali criticità per le pubbliche amministrazioni.

La realtà dei data center della pubblica amministrazione italiana, oltre ad assorbire ingenti risorse economiche, ostacola l'introduzione di tecnologie e di servizi ad alto valore che contribuirebbero all'innovazione non soltanto della pubblica amministrazione ma del Paese nel suo complesso.

Sulla base di alcune stime (ad esempio [VIV11]) è possibile ipotizzare in Italia risparmi considerevoli derivanti dall'adozione del modello cloud e da un preventivo consolidamento.

Per facilitare questa transizione, le amministrazioni dovrebbero valutare l'adozione di servizi cloud prima di rivolgersi a modalità più tradizionali di acquisizione di tecnologie IT, e dovrebbero definire una serie di servizi minimi di *governance* (come modelli decisionali, servizi di catalogo, criteri di condivisione e certificazione dei fornitori) compatibili con una possibile evoluzione dell'ecosistema IT pubblico verso un modello cloud.

Assicurare la portabilità e l'interoperabilità tra cloud diversi

Le amministrazioni dovrebbero selezionare fornitori di servizi cloud conformi agli standard e alle altre caratteristiche tecnologiche che garantiscano portabilità e interoperabilità dei servizi erogati. L'infrastruttura di un fornitore di servizi cloud deve garantire che i servizi cloud possano essere trasferiti su piattaforme di fornitori differenti ovvero possano eventualmente essere riportati all'interno dell'organizzazione cliente con il minimo di impatto, così da evitare il rischio di legarsi ad un unico cloud provider (il cosiddetto *vendor lock-in*).

I requisiti di portabilità devono essere realizzati attraverso l'adozione di standard per i diversi elementi che compongono il servizio. I principali standard di portabilità per il cloud sono:

- *Cloud Data Management Interface* (CDMI), che definisce le tipologie di interfacce che le applicazioni dovranno usare per creare, recuperare, modificare e cancellare i *data element* su un cloud (portabilità dei dati);
- *Open Virtualization Format* (OVF), che definisce lo standard per la creazione e la distribuzione delle macchine virtuali (portabilità dei sistemi).

Si sottolinea che in questo ambito gli standard possiedono differenti livelli di maturità e sono in continua evoluzione. È quindi importante fare costante riferimento alla loro evoluzione ed al loro grado di recepimento presso i primari fornitori di servizi cloud.

Promuovere l'omogeneità e la standardizzazione nelle infrastrutture e nel patrimonio applicativo

Le amministrazioni che dispongono di data center basati su pluralità di tipologie di sistemi, e che quindi non sono in grado di far condividere ai carichi elaborativi le loro risorse hardware, dovrebbero promuovere la standardizzazione delle proprie infrastrutture per assicurare la movimentazione automatica dei carichi all'interno dei propri data center.

L'omogeneità delle infrastrutture tecnologiche consente inoltre di ridurre drasticamente il numero degli addetti alla conduzione dei sistemi informativi delle Pubbliche Amministrazioni.

ENI, ad esempio, sta consolidando tutti i data center a livello mondiale utilizzando hardware a basso costo e riducendo al contempo il numero delle applicazioni ed il numero dei DBMS.

Ridefinire le competenze IT delle amministrazioni come utenti di servizi cloud

In linea di massima, l'amministrazione che fruisce di servizi cloud di tipo privato potrà mantenere (sia pure ad un livello minore) le competenze tradizionali per la gestione dei dispositivi di accesso ma dovrà acquisire competenze nuove necessarie alla corretta fruizione dei servizi cloud e alla loro integrazione con l'ambiente IT tradizionale. La fruizione di servizi cloud di tipo pubblico generalmente richiede meno competenze IT poiché le infrastrutture e le relative problematiche di gestione sono a cura del fornitore. Anche in questo modello le competenze IT prevalenti saranno legate a scenari di integrazione con le infrastrutture esistenti.

Saranno invece necessarie nuove competenze che riguardano le tematiche del trasferimento dei dati personali in altre nazioni, delle *performance* delle infrastrutture di rete di fronte a movimentazioni massicce di dati o infine dell'opportunità di ricorrere ad organizzazione terze per il controllo degli accordi contrattuali circa l'accesso ai dati o la loro cancellazione. Più in generale, sarà ancora più importante da parte delle pubbliche amministrazioni esplicitare specifiche pertinenti e complete dei servizi richiesti e, soprattutto, valutare e monitorare i fornitori e le forniture in termini di output (i risultati ottenuti) piuttosto che di input (le risorse impiegate).

RIFERIMENTI

[AMA10] Amazon: Overview of Amazon Web Services. White Paper, December 2010, http://aws.amazon.com/whitepapers

[ARP11] Fondazione Astrid e Fondazione Res Pubblica, L'impatto del cloud computing sull'economia italiana, novembre 2011, http://www.fondazionerespublica.org/wp-content/cloud20111.pdf

[AVE11] Alessandro Avenali, Modello di calcolo del TCO dell'infrastruttura di un sistema cloud, https://sps.digitpa.gov.it/sites/Cloud_Computing/Shared Documents/SG 5 - Aspetti economici, legali e contrattuali/Annual TCO Cloud Computing.xlsx

[BEL11] Ernesto Belisario, "Cloud computing" in Informatica giuridica, numero 17 eBook Altalex, 2011

[BEN08] Stefano Bendandi, Software as a Service: aspetti giuridici e negoziali, Altalex.it, 2008, http://www.altalex.com/index.php?idnot=44076.

[CAD05] D. Lgs. 82/2005 (Codice dell'Amministrazione Digitale), http://www.digitpa.gov.it/amministrazione-digitale/CAD-testo-vigente

[CAT09] D. Catteddu e G. Hogben, Cloud Computing: Benefits, Risks and Recommendations for Information Security, European Network and Information Security Agency (ENISA), 2009.00.00

[CIO] Chief Information Officers Councils in USA (www.cio.gov) e in UK (http://www.cabinetoffice.gov.uk/resource-library/chief-information-officers-council)

[CIOUS] US CIO and Federal CIO Councils, www.cio.gov

[CIP11] ICT Policy Support Programme, http://ec.europa.eu/information_society/activities/ict_psp

[CNI06] Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione, CNIPA, 2006 http://www.digitpa.gov.it/qualita_ict/le-linee-guida

[CNI08] Relazione annuale sullo stato dell'ICT nella PAC, CNIPA, 2008 e Indagine CNIPA 2006

[CONSIP] Matteo Cavallini, Cloud security: una sfida per il futuro, Quaderni CONSIP, II/2011, http://www.consip.it/on-line/Home/Pressroom/QuaderniConsip/QuaderniConsip2011/documento6416.html.

[COST] Costituzione della Repubblica Italiana, http://www.quirinale.it/qrnw/statico/costituzione/costituzione.htm

[CSA10] Top Threats to Cloud Computing, Cloud Security Alliance, 2010 https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[CSACAI11] Consensus Assessments Initiative, Cloud Security Alliance, https://cloudsecurityalliance.org/research/initiatives/cai

[CSACCM11] Cloud Control Matrix, Cloud Security Alliance, https://cloudsecurityalliance.org/research/initiatives/ccm

[CSW11] Cloud Standards Wiki, http://cloud-standards.org

[DAE10] Un'agenda digitale per l'Europa, COM(2010) 245 def/2, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:IT:PDF

[DGI10] The Future of Cloud Computing - Opportunities for European Cloud Computing beyond 2010 Expert Group Report, EU Commission – DG INFSO, 2010 http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

[DIG11] DigitPA, Linee guida per il disaster recovery delle pubbliche amministrazioni, 2011, http://www.digitpa.gov.it/sites/default/files/LINEE%20GUIDA%20PER%20IL%20DISASTER%20RECOVERY%20DELLE%20PA_0.pdf

[DMTF11] Open Virtualization Format (OVF), DMTF Inc., http://www.dmtf.org/standards/ovf

[EC10] European Commission - Expert Group Report: The Future Of Cloud Computing. Opportunities For European Cloud Computing Beyond 2010, Ed. Keith Jeffery, Burkhard Neidecker-Lutz.

[ENIGDC] Programma Green Data Center, ENI, http://www.eni.com/green-data-center/it_IT/pages/home.shtm

[ENISA09] Cloud Computing - Benefits, risk and recommendations for information security, ENISA, Novembre 2009

[ENISAIAF09] Information Assurance Framework, ENISA, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework

[ENISASR09] Cloud Computing Security Risk Assessment, ENISA, November 2009, http://www.enisa.europa.eu/publications/studies/reports/act/rm/files/deliverables/cloud-computing-risk-assessment

[ENISASR11] Security and Resilience in governmental cloud, ENISA, http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds

[ERC10] ERCIM NEWS: Special theme: Cloud Computing, October 2010

[ETR09] Federico Etro, The economic impact of cloud computing on business creation, Review of Business and Economics 54(2):179-208, http://www.intertic.org/Policy%20Papers/RBE.pdf

[EUAP10] European eGovernment Action Plan 2011 – 2015 COM(2010) 743 15 December 2010 http://ec.europa.eu/information_society/activities/egovernment/action_plan_2011_2015/index_en.htm

[GAR10] Cloud Computing: indicazioni per l'utilizzo consapevole dei servizi, Garante per la protezione dei dati personali, 2010 http://www.garanteprivacy.it/garante/document?ID=1819933

[GART10] Andrea Di Maio, Government and the Cloud: the Truth behind the Hype, Gartner Group, 2010 http://www.gartner.com/it/content/1418100/1418123/september_8_government_cloud_truth_behind_hype.pdf

[GART11] Gartner Group, Public Cloud Services Forecast, Worldwide, 2Q11 Update.

[HOE10] C. N. Hoefer, G. Karagiannis: Taxonomy of cloud computing services. In Proceedings of GLOBECOM Workshops (GC Wkshps), 2010 IEEE, pages 1345 - 1350

[IIPP11] "Cloud computing e tutela dei dati personali in Italia: una sfida d'esempio per l'Europa", in *Diritto, Economia e Tecnologie della Privacy,* Settembre 2011*,* Istituto Italiano per la Privacy.

[IND11] Industry Recommendations to Vice Presidente Neelie Kroes On The Orientation Of A European Cloud Computing Strategy, November 2011 http://ec.europa.eu/information_society/activities/cloudcomputing/docs/industryrecommendations-ccstrategy-nov2011.pdf

[ISA11] ISA Programme – Interoperability Solutions for European Public Administrations, http://ec.europa.eu/isa

[KRO11] Neelie Kroes, Towards a European Cloud Computing Strategy, discorso al World Economic Forum, Davos, 27 gennaio 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/50

[KRO12] Neelie Kroes, Setting up the European Cloud Partnership, discorso al World Economic Forum, Davos, 26 gennaio 2012, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/38

[MAL09] Malmö Declaration, http://www.egov2009.se/wp-content/uploads/Ministerial-Declaration-on-eGovernment.pdf

[MSI11] Microsoft Integrated Virtualization ROI Tool, https://roianalyst.alinean.com/microsoft/virtualization

[NIST11] P. Mell, T. Grance: The NIST Definition of Cloud Computing. Recommendation of the National Institute of Standards and Technology (NIST), U.S. Department of Commerce, January 2011

[NISTCCRA11] NIST Cloud Computing Reference Architecture, September 2011 http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909505

[NISTCON11] Technical Considerations for US Government Cloud Computing Deployment Decisions, NIST, http://www.nist.gov/itl/cloud/upload/NIST_cloud_roadmap_VIII_draft_110111-v3_rbb.pdf

[NISTDOC] Cfr. Documentazione del NIST, http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/Documents

[NISTR11] L. Badger, D. Bernstein, R. Bohn, F. de Vaulx, M. Hogan, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside and D. Leaf: US Government Cloud Computing Technology Roadmap Volume I Release 1.00 (Draft). High-Priority Requirements to Further USG Agency Cloud Computing Adoption. NIST Cloud Computing Program Information Technology Laboratory. November 2011

[NISTR11a] L. Badger, D. Bernstein, R. Bohn, F. de Vaulx, M. Hogan, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside and D. Leaf: US Government Cloud Computing Technology Roadmap Volume II Release 1.00 (Draft). Useful Information for Cloud Adopters. NIST Cloud Computing Program Information Technology Laboratory. November 2011

[NISTR11b] NIST SAJACC and BUC Working Groups: NIST US Government Cloud Computing Technology Roadmap Volume III. Technical Considerations for USG Cloud Computing Deployment Decisions. First Working Draft, November 2011

[NISTSTD11] Cloud Computing Standards Roadmap, NIST, July 2011 http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/StandardsRoadmap/NIST_SP_500-291_Jul5A.pdf

[NISTSYN11] DRAFT Cloud Computing Synopsis and Recommendations, NIST, May 2011 http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

[RAND11] The Cloud – Understanding the Security, Privacy and Trust Challenges, RAND Technical Reports, 2011 http://www.rand.org/pubs/technical_reports/TR933.html

[REA11] J. Reavis e D. Catteddu, Cloud Security Alliance Contribution to the European Commission Strategy on Cloud Computing, November 2011 https://cloudsecurityalliance.org/wp-content/uploads/2011/11/CSA_EU_Response_Final.pdf

[SUN09] Sun Microsystems: Introduction to Cloud Computing Architecture, White Paper, 1st Edition, June 2009

[UKICT] UK Government ICT Strategy resources, http://www.cabinetoffice.gov.uk/resource-library/uk-government-ict-strategy-resources

[ULS11] Carta di Castelfranco - Raccomandazioni per i consumatori di cloud computing di sanità digitale, ULSS 8 Asolo e ForumPA, Castefranco Veneto, ottobre 2011 www.ulssasolo.ven.it

[VAQ09] L. M. Vaquero, L. Rodero-Merino, J. Caceres, M. Lindner: A Break in the Clouds: Towards a Cloud De?nition. ACM SIGCOMM Computer Communication Review, Volume 39 Number 1 January 2009

[VIV10] Vivek Kundra, US Chief Information Officer, 25 Point Implementation Plan to Reform Federal Information Technology Management, http://www.cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf

[VIV11] Vivek Kundra, US Chief Information Officer, Federal Cloud Computing Strategy, http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

[VMW11] VMware, ROI TCO Calculator, http://roitco.vmware.com/vmw/Content/VMware_ROI_TCO_Calculator_Guide.pdf

[WEF10] Advancing Cloud Computing: What to do now ?, World Economic Forum, 2010, http://www.weforum.org/reports/advancing-cloud-computing-what-do-now