federalismi.it
Rivista di diritto pubblico italiano, comunitario e comparato

DATI NELLE NUVOLE: ASPETTI GIURIDICI DEL *CLOUD COMPUTING* E APPLICAZIONE ALLE AMMINISTRAZIONI PUBBLICHE[*]

di

Caterina Flick

(Avvocato in Roma e Docente di diritto dell'informatica)

e

Vincenzo Ambriola

(Professore ordinario di Informatica
Università di Pisa)

20 marzo 2013

Sommario: **1.** Introduzione al *cloud computing*: definizioni, modelli e servizi offerti. **2.** Vantaggi e rischi del *cloud computing*. **3.** Disponibilità e sicurezza nel *cloud computing*. **4.** La proprietà dei dati e la tutela dei dati personali. **5.** La proprietà delle infrastrutture e del software: *open cloud*. **6.** Il rapporto tra utente e fornitore. **7.** Il *cloud computing* nelle pubbliche amministrazioni: le indicazioni dell'Europa. **8.** Il *cloud computing* nelle pubbliche amministrazioni: l'approccio italiano. **9.** Dimensione politica del *cloud computing* ed esigenze di armonizzazione

[*] Articolo sottoposto a referaggio. Il presente lavoro è il risultato di una ricerca interdisciplinare che, per la sua natura, ha richiesto il contributo di studiosi dell'area giuridica e dell'area informatica. Il paragrafo 1 è riconducibile all'elaborazione esclusiva di Vincenzo Ambriola, i paragrafi da 2 a 8 sono riconducibili all'elaborazione esclusiva di Caterina Flick.

1. Introduzione al *cloud computing*: definizioni, modelli e servizi offerti

1.1 - definizioni

Il termine *cloud computing* è usato per definire le tecnologie che consentono la delocalizzazione di risorse e servizi informatici. Il NIST (National Institute of Standards and Technology) definisce il *cloud computing* come un modello che abilita l'accesso tramite internet a risorse condivise di calcolo, utilizzabili dinamicamente ed efficacemente a fronte di limitate attività di gestione.

Pur basandosi su tecnologie oramai mature e consolidate, il *cloud computing* costituisce un paradigma moderno mediante il quale gestire risorse ed erogare servizi informatici. In particolare, il *cloud computing* è utilizzato per servizi a erogazione diffusa (quali posta elettronica o *social network*) diretti a singoli, imprese o pubbliche amministrazioni. In un'accezione più ampia, il termine è utilizzato per indicare la fornitura di servizi rivolti all'automazione dei processi di gestione delle attività di impresa e alla gestione d'ufficio.

1.2 – modelli e caratteristiche comuni

Tra i modelli attualmente esistenti si suole distinguere tra *private*, *pubblic* e *community cloud*, tenendo conto dell'utenza a cui è rivolta la fornitura dei servizi e l'uso delle risorse. Questi modelli differiscono essenzialmente per le caratteristiche dell'*infrastruttura informatica* utilizzata.

Nel caso del *private cloud*, l'infrastruttura è dedicata alle esigenze di un'unica organizzazione e può essere gestita in proprio (*in house*) oppure da un soggetto esterno (un semplice *hosting server* oppure un vero e proprio *outsourcer*). Il *private cloud* permette di consolidare l'infrastruttura e le applicazioni informatiche necessarie per la gestione delle risorse e l'erogazione dei servizi, a vantaggio di un significativo aumento di efficienza ed efficacia. La scelta delle tecnologie da adottare è affidata al responsabile informatico delle singole organizzazioni, si tratti di soggetti privati o di soggetti pubblici.

Nel caso del *public cloud*, l'infrastruttura è proprietà di un fornitore specializzato in questo ambito tecnologico. Il fornitore mette a disposizione degli utenti, e quindi condivide tra di loro, la propria infrastruttura garantendo l'erogazione via web di servizi, di capacità di calcolo e di memorizzazione permanente. Il *public cloud* è rivolto a una platea di utenti, che – in molti casi – non hanno alcun rapporto tra di loro.

Nel *community cloud* l'infrastruttura è utilizzata da utenti che hanno elementi comuni: una specifica comunità nel cui ambito si condividono particolari obiettivi o esigenze (ad esempio finalità, requisiti di sicurezza, politiche di gestione). L'infrastruttura può essere gestita dalla

stessa comunità o da un soggetto esterno e può essere organizzata come una rete. Il *community cloud* è sovente ritenuto il modello che più corrisponde alle esigenze della pubblica amministrazione, intesa come insieme di organizzazioni distinte che operano in uno stesso contesto giuridico/amministrativo, che hanno analoghi requisiti di sicurezza, di conformità e di politiche di gestione e che possono così interoperare in maniera più efficace, imponendo – se del caso – al fornitore di adottare *standards* di sicurezza adeguati alle esigenze. [1]

Esistono infine modelli ibridi, detti anche *intermediate cloud*, nei quali l'infrastruttura è composta da due o più tipi di *cloud*, separati tra loro, ma che condividono standard o tecnologie per la portabilità dei dati e l'interoperabilità delle applicazioni. Trattandosi di modelli derivanti dalla combinazione di più tipologie di *cloud*, si può assumere che un ibrido rappresenti il secondo passo nell'approccio al *cloud computing*; una possibile configurazione ibrida può, ad esempio, prevedere l'utilizzo di servizi erogati da strutture private accanto a servizi acquistati da *cloud* pubblici.

Le caratteristiche principali del *cloud computing*, comuni ai diversi modelli, possono essere così schematizzate: i dati elaborati e memorizzati nell'infrastruttura non risiedono fisicamente su risorse di calcolo dell'utente, ma del fornitore; l'infrastruttura è (o può essere) condivisa tra molti utenti, per cui è fondamentale da parte del fornitore l'adozione di sistemi di sicurezza che garantiscano la riservatezza dei dati e controllino i diritti di accesso all'infrastruttura; l'accesso all'infrastruttura avviene via web tramite internet, che assume dunque un ruolo centrale in merito al livello di qualità dei servizi fruiti e offerti; i servizi sono acquisibili a consumo dal fornitore, che può affrontare efficacemente le situazioni eccezionali in cui sono necessarie risorse aggiuntive rispetto a quelle utilizzate di norma.

1.3 – servizi

I servizi offerti dall'infrastruttura, in particolare da quella tipica del *public cloud*, possono essere a loro volta suddivisi in tre tipologie: *Infrastructure as a Service* (IaaS), *Software as a Service* (SaaS), *Platform as a Service* (PaaS).

Nel primo caso – IaaS - il fornitore mette a disposizione un'infrastruttura in sostituzione o in aggiunta a sistemi che l'utente ha già a disposizione. In questo caso le risorse messe a

[1] La scelta del modello più efficace per la pubblica amministrazione (in particolare *private* o *community cloud*) può richiedere l'individuazione di un ruolo di responsabile informatico generale a livello di governo centrale, che attualmente in Italia non esiste.

disposizione dell'utente, non sono predefinite a priori, ma individuate di volta in volta, a seconda delle effettive esigenze che si presentano al momento.

Nel secondo caso – SaaS - il fornitore eroga direttamente i servizi, spesso in sostituzione di quelli già installati dagli utenti sui loro sistemi. Tra i più diffusi vi sono fogli di calcolo e strumenti di elaborazione dei testi, applicazioni per il protocollo informatico, rubrica dei contatti, calendari condivisi, sistemi di posta elettronica.

Nel terzo caso – PaaS - il fornitore offre gli strumenti per sviluppare e ospitare le applicazioni. Generalmente questa modalità è rivolta a operatori di mercato che sviluppano in proprio applicazioni mirate sia all'assolvimento di esigenze interne che alla fornitura di servizi a terzi. Il vantaggio consiste anche nel fatto che l'utente non si deve dotare di proprie risorse di calcolo o di applicazioni specifiche o aggiuntive. L'utente che usufruisce di questi strumenti non ha il controllo diretto dell'infrastruttura, a meno che non abbia a disposizione una piattaforma informatica che può gestire direttamente: in questo caso si configura una sorta di *private cloud* gestito direttamente dall'utente.

2. Vantaggi e rischi del *cloud computing*

2.1 – Vantaggi

Dal punto di vista dell'utente diversi sono i vantaggi dell'utilizzo del *cloud computing*.

Poiché le risorse e le applicazioni sono direttamente accessibili via internet, l'utente che se ne avvale non deve acquisire beni caratterizzati da una rapida obsolescenza, ma può ottenerli sotto forma di servizio; gli utenti non devono occuparsi direttamente della gestione dell'infrastruttura, lasciando tale compito a terzi; i dati possono essere trattati in remoto tramite internet e generalmente senza dover installare in locale applicazioni specifiche; è possibile disporre di spazi di memoria, anche di grandi dimensioni, dove archiviare i propri documenti senza utilizzare supporti esterni.

Infine, il fatto che le risorse, comprese le infrastrutture necessarie per rendere disponibili i servizi, siano generalmente condivise tra molti utenti, permette di ottenere economie di scala e di garantire elevati livelli di sicurezza a costi ragionevoli.

2.2 – rischi

Il prezzo da pagare per ottenere i vantaggi sopra elencati sta nella necessità di trasformare in servizi erogati da altri delle attività in precedenza gestite in proprio. Ciò comporta, per l'utente, una potenziale perdita di controllo sui dati propri o trattati per conto terzi (clienti, cittadini e quant'altro), nonché la cessione di un potere notevole nelle mani del fornitore. Più

in generale, se vi sono pochi soggetti (società multinazionali) idonei a erogare i servizi, si corre il rischio di concentrare nelle loro mani un'ingente e preziosa quantità di dati (i c.d. *Big Data*).

Come anticipato, poiché l'utente può accedere via internet ai suoi dati, le risorse fisiche in cui questi dati sono effettivamente conservati risiedono in un luogo diverso da quello da cui avviene l'accesso. La complessità dell'infrastruttura, nonché la sua dislocazione in luoghi sconosciuti all'utente - anche al di fuori dei confini nazionali - oltre a determinare difficoltà oggettive nell'individuazione dell'esatto luogo di conservazione dei dati, rende difficile anche l'esatta conoscenza del loro spostamento da una sede all'altra, per esigenze di carattere organizzativo, tecnico o economico del fornitore. L'utente non può, quindi, sapere dove si trovino in un certo momento i dati trattati dall'infrastruttura e se la normativa del paese in cui l'infrastruttura è fisicamente ospitata garantisce il rispetto dei diritti tutelati nel paese ove egli risiede.

In secondo luogo, le caratteristiche di qualità dell'infrastruttura devono essere tali da assicurare sia la disponibilità continuativa dei servizi che la sicurezza dei dati. Ne consegue la necessità di garantire - e rispettivamente di assicurarsi – che a fronte di una specifica richiesta da parte dell'utente vi siano da un lato la disponibilità del servizio, dall'altro l'accessibilità dei dati.

È inoltre indispensabile assicurare la riservatezza dei dati rispetto ad accessi non autorizzati; ciò – a tacer d'altro - in considerazione del fatto che generalmente i fornitori custodiscono dati di singoli o di organizzazioni diverse, che potrebbero avere esigenze o interessi differenti, se non addirittura contrastanti

Infine, l'adozione da parte del fornitore di proprie tecnologie (*close source*) può non garantire l'interoperabilità con altre infrastrutture, rendendo complessa per l'utente la portabilità dei dati e lo scambio di informazioni con soggetti che utilizzano servizi di fornitori differenti. A questo proposito non si può trascurare il fatto che l'eventuale fornitura dei servizi di *cloud computing* da parte di pochi soggetti può determinare anche un aumento dei costi connessi al passaggio da un fornitore all'altro e da un modello a uno differente.

3. Disponibilità e sicurezza nel *cloud computing*

3.1 – disponibilità e accessibilità

La disponibilità dei dati, e la loro accessibilità in qualunque momento, richiede in primo luogo la certezza sui livelli di qualità della connettività forniti da internet. In caso contrario, il servizio potrebbe essere degradato da picchi di traffico o, addirittura, reso indisponibile da

eventi anomali (guasti, ad esempio). Questo aspetto dipende solo in parte dai fornitori di *cloud computing*, mentre coinvolge in pieno gli organi politici e di governo, responsabili di scelte che possono avere grande influenza sulla di organizzazione, diffusione e gestione di internet, quali, ad esempio, le problematiche relative agli investimenti necessari per la diffusione della banda larga.

L'accessibilità dei dati (personali, documentali) richiede per altro verso di preservarne l'integrità, assicurandoli rispetto alla cancellazione o al danneggiamento; è necessaria inoltre l'adozione di misure di sicurezza idonee a tutelare la riservatezza dei dati, rispetto alla visibilità o all'utilizzo da parte di soggetti non autorizzati. Anche se il rispetto della riservatezza dei dati dipende in gran parte dai meccanismi di sicurezza adottati dal fornitore, ciò non esime i soggetti pubblici e privati che se ne avvalgono per la gestione del proprio patrimonio informativo o - a maggior ragione - di dati e informazioni per conto di terzi, dalle responsabilità loro attribuite, nella misura in cui debbano attivarsi per l'adozione di opportune misure volte alla sicurezza dei dati e dei sistemi informatici all'interno della propria struttura[2].

3.2 – sicurezza

Da parte del fornitore è essenziale garantire in modo trasparente la sicurezza dei dati, curandone correttamente la trasmissione e la conservazione, ivi compresa l'adozione di meccanismi sicuri di salvataggio periodico. Qualunque aspetto tecnico e organizzativo dell'infrastruttura - dalla sua progettazione globale, al processo di sviluppo dei servizi erogati, alla configurazione dei sistemi di trasmissione, all'impostazione dei contratti con utenti e subappaltatori, ai sistemi di controllo delle richieste di accesso - ha un ruolo essenziale nell'obiettivo finale di garantire la sicurezza dei dati.

L'esigenza di tutelare i dati da intrusioni e utilizzi illeciti – che richiede di limitare la quantità di informazioni relative agli utenti, al traffico, alla struttura, che restano utilizzabili – può porsi in contrasto con la necessità sia di rendere i dati rapidamente e continuativamente disponibili agli utenti, sia di reagire prontamente in caso di emergenza. Questa esigenza si contrappone anche con le esigenze di riservatezza (o meglio con l'interesse a non essere controllati) di coloro che sono autorizzati ad accedere. In caso di difficoltà, infatti, l'accuratezza e la tempestività della diagnosi e del rimedio sono strettamente connesse con la

[2]Nel caso del trattamento di dati personali l'utente di un'infrastruttura di *cloud computing* resta responsabile dell'adozione di misure di sicurezza, nella misura in cui riveste la qualifica di "titolare" del trattamento. Si pensi, inoltre, agli obblighi in materia di sicurezza informatica connessi con la responsabilità amministrativa delle imprese in caso di commissione di reati informatici al loro interno.

completezza delle informazioni disponibili. Inoltre, poiché molti errori e anomalie coinvolgono fornitori diversi, la risoluzione di un problema può richiedere la collaborazione tra più soggetti, potenzialmente residenti in stati diversi.

In sintesi, un sistema che tutela la sicurezza e la riservatezza dei dati ha due obiettivi: da un lato deve essere in grado di individuare un attacco con accuratezza e il più rapidamente possibile e deve reagire altrettanto rapidamente, per salvaguardare i livelli di qualità dei servizi erogati; dall'altro deve garantire la riservatezza degli utenti coinvolti e le cui azioni sono monitorate.[3]

4. La proprietà dei dati e la tutela dei dati personali

4.1 – proprietà dei dati

L'affidamento del trattamento dei dati al fornitore di servizi di *cloud computing* richiede di definire preliminarmente il rapporto di titolarità – o proprietà – con i dati affidati. A questo proposito si pone, in primo luogo, il tema dei diritti di proprietà intellettuale e industriale, con le possibili difficoltà di farli valere a fronte dell'evidenziata difficoltà di individuare il luogo in cui tali dati vengono immagazzinati.

Con particolare riferimento alle opere creative vale segnalare che la dematerializzazione dei supporti e la conservazione delle opere stesse presso il fornitore (su supporti di proprietà del fornitore) può cambiare le modalità di fruizione delle opere stesse, che potrebbero essere messe a disposizione di diversi utenti, attraverso un accesso *on demand* da più postazioni, su autorizzazione dell'autore dell'opera, ma anche a sua insaputa.

Per altro verso, la riunificazione di dati nelle mani di singoli operatori di mercato che non intervengono nel mettere a disposizione su internet opere creative ma che si limitano a consentirne la diffusione richiede, sotto il profilo della tutela dell'autore dell'opera, la necessità di abbattere l'ampio ambito di irresponsabilità del fornitore del servizio, che consente a quest'ultimo di non rispondere per i contenuti caricati dagli utenti. È evidente, infatti, la difficoltà per l'autore dell'opera di individuare i singoli che, in ipotesi, abbiano

[3] A fronte di una riduzione dei dati relativi agli utenti si può aumentare il livello di riservatezza, pur garantendo le operazioni di ripristino dell'infrastruttura; analogamente, all'aumentare dei dati disponibili, può essere elevato il livello di protezione. Una soluzione in grado di sciogliere questo dilemma si basa sull'uso di tecniche avanzate di crittografia.

violato i suoi diritti (alla quale si aggiungono problemi di coordinamento con la disciplina in materia di privacy) e costi considerevoli che un'indagine su singoli soggetti comporterebbe [4].
In mancanza di modifiche normative tra gli obblighi che gravano su un prestatore di servizi di *cloud computing*, assimilabili in questo senso agli altri fornitori di servizi su internet, vi è solo quello di informare l'autorità giudiziaria o amministrativa di vigilanza, relativamente a notizie attendibili ricevute in ordine alla violazione di diritti d'autore compiute attraverso la propria rete di telecomunicazione e non anche l'obbligo di interrompere il servizio prestato a favore di soggetti di cui abbia avuto notizia in ordine ad atti illeciti di messa a disposizione di contenuti lesivi di diritti d'autore[5].

4.2 – trattamento dei dati personali

Un altro profilo di grande importanza da considerare quando si affrontano le tematiche relative al *cloud computing* attiene alle esigenze connesse al trattamento dei dati personali; ciò sia durante il rapporto contrattuale, sia al termine di esso, in relazione agli obblighi di distruzione dei dati detenuti dal fornitore. In linea generale è sufficiente dire che i principi previsti in materia di tutela dei dati personali devono essere adattati all'utilizzo dei servizi di *cloud computing*, tenendo cioè conto delle problematiche connesse con le peculiarità di tali sistemi. Più in particolare è necessario affrontare il tema degli obblighi posti in capo al fornitore, in quanto soggetto diverso dal titolare del trattamento, e nominato da quest'ultimo responsabile, in presenza di vasti poteri nel trattamento in concreto dei dati stessi.
La questione deve essere affrontata con particolare attenzione nel caso in cui i dati affidati alla gestione del fornitore dell'infrastruttura da parte dell'utente – titolare del trattamento - riguardano terzi interessati: è questo il caso, ad esempio, della pubblica amministrazione, che tratta i dati dei cittadini, oltre a quelli dei propri dipendenti.
Una seconda problematica è connessa con il tema del trasferimento dei dati all'estero, in particolare nel caso in cui le risorse di calcolo siano fisicamente allocate in paesi situati al di

[4] Il conflitto fra i diversi interessi è stato portato nelle aule giudiziarie italiane, con la cd. Vicenda *peppermint*, che ha visto contrapporsi la tutela del diritti d'autore, di cui era portatrice la casa discografica Peppermint, con la tutela della privacy degli utenti di internet.
[5] In Italia la responsabilità del prestatore di servizi su internet si fonda essenzialmente sul d.lgs. 70/2003 (recepimento della direttiva 31/00), che esclude la responsabilità del fornitore che non intervenga nelle attività degli utenti, nonché un suo generale obbligo di sorveglianza sui dati trasmessi, imponendogli però di denunciare attività illecite di cui sia comunque venuto a conoscenza, fornendo le informazioni dirette all'identificazione dell'autore dell'attività illecita.
La giurisprudenza recente tuttavia – e non solo quella italiana – si sta orientando verso una estensione del concetto di "intermediazione" del fornitore: così il contenzioso sulla diffusione su internet di trasmissioni televisive, che ha visto contrapporsi Mediaset e Yahoo innanzi ai Tribunali italiani e alla Corte di Giustizia UE, e il contenzioso sulla vendita di materiale contraffatto, che ha visto contrapporsi Christian Dior Couture e E-Bay

fuori dei confini dell'Unione Europea. Come è noto, la normativa comunitaria in proposito consente la trasmissione di dati in paesi terzi solo se è garantito un adeguato livello di protezione (eventualmente sarà necessario avere il consenso dell'autorità nazionale che dovrà valutare l'adeguatezza della tutela che le parti si apprestano a garantire sulla base degli accordi negoziali pattuiti, ai sensi della vigente normativa europea sul trattamento dei dati personali). Le verifiche e gli adempimenti in tal senso - che dovranno precedere il trasferimento dei dati - saranno agevoli ove vi sia un rapporto diretto tra l'utente e il fornitore, o sub-fornitore, residente al di fuori del territorio dell'Unione Europea, saranno più complessi ove intervengano più soggetti nella fornitura di servizi di *cloud computing*.

Un terzo aspetto che merita attenzione è connesso con la possibilità che un'ingente quantità di dati - forniti da diversi titolari, portatori di interessi diversi - siano trattati da un limitato numero di società multinazionali, con possibili rischi di commistioni e conflitti.

4.3 – esigenze di armonizzazione normativa

L'uso del *cloud computing* può beneficiare molto dell'armonizzazione delle norme sul trattamento, la conservazione e la protezione dei dati, sulla base di una regolamentazione comune, che preveda anche politiche che facilitino l'effettiva applicazione delle norme.

Sul tema della protezione dei dati rispetto ad aggressioni ai sistemi informatici diversi principi sono contenuti nella Convenzione del Consiglio d'Europa sul *cybercrime*, firmata a Budapest nel 2001 e , e riguardante i crimini commessi attraverso internet o altre reti informatiche si può richiamare la convenzione di Budapest sul *cybercrime* del 2001, recepita da diversi paesi europei ed extraeuropei[6]. Tra gli obiettivi fondamentali che si pone la Convenzione, vi è quello di armonizzare gli elementi fondamentali delle fattispecie di reato previste dai singoli ordinamenti interni e tutte le disposizioni riguardanti la criminalità informatica, al fine di perseguire tutti i reati in qualunque modo commessi attraverso o a danno di un sistema informatico e quelli di cui si debbano o possano raccogliere prove in forma elettronica. L'ambito di applicazione comprende gli atti che comportano l'aggressione alla segretezza, integrità e disponibilità dei sistemi informatici, delle reti e dei dati, così come l'uso fraudolento di tali sistemi, reti e dati.

Sul tema della tutela del diritto d'autore, e dell'eventuale responsabilità dei fornitori in caso di violazioni, il dibattito è ancora aperto sia in ambito europeo che nazionale.

[6] In Italia la Convenzione di Budapest è stata ratificata con L. 48/08 ed ha, tra l'altro si veda, in particolare, la previsione di introdotto una specifica responsabilità per le imprese per i reati informatici compiuti al loro interno e sui loro sistemi informatici, contenuta nel d.lgs. 231/01.

Sul tema della protezione dei dati personali l'Unione Europea si sta muovendo, tenendo conto della diffusione di sistemi portabili e di reti. È infatti in corso di approvazione un regolamento che interviene a modificare la direttiva 95/46 sulla protezione dei dati personali. Il regolamento, in primo luogo introduce la figura del responsabile della sicurezza dei dati, accanto alle figure – titolare, responsabile, incaricato – già previste dalla normativa vigente. In secondo luogo sono posti in capo ai fornitori obblighi di segnalazione, agli interessati e alle locali autorità garanti, delle eventuali violazioni della sicurezza dei dati. In terzo luogo il regolamento prevede l'applicazione delle norme europee (e la giurisdizione europea) al caso in cui il trattamento comporti la fornitura di servizi a soggetti residenti nell'Unione Europea[7]. Nell'attesa della definitiva approvazione del regolamento – e della sua efficacia in ambito nazionale – occorre applicare le norme vigenti, tenendone conto nella stipula dei contratti. In particolare può essere opportuno prevedere clausole che tengano in considerazione l'ipotesi di trasferimento dei dati in paesi al di fuori dell'Unione Europea, specie in quei paesi ove manca una legislazione idonea ad assicurare un adeguato livello di protezione dei dati personali in conformità con quanto previsto dalla legislazione europea, vietando il trasferimento o prevedendo nel dettaglio clausole contrattuali adeguate.

5. La proprietà delle infrastrutture e del software: *open cloud*

Nel corso del tempo può presentarsi la necessità di cambiare fornitore, determinata da cambiamenti strutturali dell'utilizzatore (fusioni o acquisizioni societarie), dal mutamento delle esigenze o da modifiche normative. Ciò richiede di preoccuparsi – alla stipula di un contratto per servizi di *cloud computing* - della portabilità dei dati, sotto il duplice profilo del loro recupero (che richiede la conoscibilità dei sistemi) e della loro piena riutilizzabilità. Tali aspetti sono connessi da un lato con le caratteristiche tecniche, dall'altro con le licenze d'uso delle applicazioni informatiche utilizzate dal fornitore.

Il ricorso a un diverso fornitore o a una diversa infrastruttura potrebbe essere agevolato dall'utilizzo di un *open cloud* (in sintesi un *cloud* realizzato con tecnologia *open source*) che, per le sue caratteristiche di flessibilità (sotto il profilo hardware e software) e conoscibilità, può facilitare il processo di migrazione.

I fautori dell'*open cloud* - riproponendo temi già ampiamente discussi in altre sedi - evidenziano che le infrastrutture di *cloud computing* fornite come *close source* oppure come *open source* interni non permettono alla comunità di contribuire al loro sviluppo, rendendo

[7] tali previsioni sono analoghe a quelle già introdotte con riferimento alla fornitura di servizi di comunicazione elettronica.

complicate convergenza e interoperabilità, anche perché le tecnologie sono conosciute solo da alcuni professionisti specializzati. L'utilizzo dell'*open cloud*, consentirebbe invece di ovviare al problema, permettendo inoltre di individuare facilmente professionisti competenti.

Nell'*open cloud*, in primo luogo, il fatto che i fornitori lavorino insieme assicura che le caratteristiche scelte (sicurezza, integrazione, portabilità, interoperabilità, *governance/managment*, monitoraggio) sono indirizzate verso una collaborazione aperta e verso l'uso appropriato degli standard. In secondo luogo, i fornitori non utilizzano la propria posizione di mercato per vincolare gli utilizzatori a particolari piattaforme, né limitano la loro scelta tra fornitori. In terzo luogo, i fornitori devono, e possono, utilizzare e adottare standard esistenti e appropriati: non hanno la necessità di duplicare né di reinventare tecnologie; quando si rende necessario l'utilizzo di nuovi standard o la modifica di quelli esistenti, gli sviluppatori si assicurano di non crearne troppi e del fatto che i nuovi standard promuovono e non inibiscono l'innovazione. In quarto luogo, lo sforzo della comunità che si muove intorno a un *open cloud* è diretta a perseguire i bisogni degli utilizzatori e dovrebbe essere verificata rispetto alle loro reali esigenze.

Qualunque sia la scelta dell'utente, i criteri enunciati possono essere tenuti presenti per assicurarsi che un'infrastruttura di *cloud computing* sia aperta e consenta la scelta, la flessibilità e l'agilità richieste dall'utilizzatore.

Nella pratica, dalle statistiche pubblicate sui siti web delle comunità *open source* emerge che l'utilizzo di infrastrutture di *open cloud* non è esclusivamente limitato all'utilizzo nelle comunità di ricerca per la pubblicazione dei risultati di progetto, ma è anche destinato agli utilizzatori finali. Anche le pubbliche amministrazioni europee fanno ricorso a soluzioni *open source* a supporto delle proprie attività.

In Europa vi sono anche ampie comunità di sviluppo e un forte *background* nello sviluppo e nell'utilizzo dell'*open source*. Tuttavia, molte tecnologie sviluppate in Europa sono sfruttate da società statunitensi: stando alle stime, il 90% del volume di affari derivante da sistemi *open source* è generato da utenti non europei; ancora, molti consorzi che si occupano dello sviluppo e della commercializzazione dell'*open source* hanno sede negli Stati Uniti e sono state fondate da società IT statunitensi (come Sourceforge e Code Plex).

Se la ricerca sul *cloud computing* ha come obiettivo la realizzazione di un'opportunità economica europea sostenibile (cfr. ultra), è opportuno un maggiore sviluppo delle aziende europee con diversi modelli imprenditoriali, volte a sviluppare al meglio questo patrimonio tecnologico.

6. Il rapporto tra utente e fornitore

6.1 – accordi contrattuali

L'utilizzo dei sistemi di *cloud computing* comporta l'instaurarsi di un rapporto complesso tra utente e fornitore che richiede normative adeguate, sia a livello locale che sovranazionale. A fronte di una regolamentazione normativa scarsa e poco uniforme diviene essenziale la stipula di accordi tali da disciplinare tutti gli aspetti relativi alla fornitura dei servizi e alla gestione dei dati, tra i quali modalità, durata e particolarità del trattamento. Ciò non è possibile ove si acceda a servizi già esistenti e forniti con il sistema dei contratti c.d. "per adesione", nei quali le clausole contrattuali sono uniformate e spesso non definiscono aspetti delicati (quali responsabilità, livelli di servizio, legge applicabile ecc.)

L'importanza di disciplinare nel dettaglio le modalità e le condizioni del servizio è, invece, di estrema rilevanza anche per il fatto che nel *cloud computing* entrano in gioco diversi soggetti (il gestore del servizio, i fornitori di accesso a internet) e da ciascuno di questi sarà necessario ricevere opportune informazioni e garanzie contrattuali, circa i parametri qualitativi del servizio prestato.

Le responsabilità derivanti dalla fornitura di servizi di conservazione digitale devono essere previste da un'analisi a monte che rifletta nel relativo contratto i termini delle responsabilità poste a in capo sia al fornitore del servizio; sia a eventuali intermediari (che concorrono all'erogazione del servizio finale) o al responsabile della conservazione (inteso quale persona giuridica a cui delegare parte dei processi, compresi quelli relativi all'archiviazione delle informazioni nell'infrastruttura di *cloud computing*), poiché la conservazione dei dati in luoghi geografici differenti potrebbe avere riflessi sia sulla normativa applicabile in caso di contenzioso tra il titolare del dato e il fornitore; sia in relazione alla specifica legge nazionale che disciplina il trattamento, l'archiviazione e la sicurezza dei dati. Di conseguenza, nel gestire al meglio la contrattualizzazione del servizio di *cloud computing* applicato ai processi di conservazione digitale risulta fondamentale l'applicazione di quel concetto di "interoperabilità intellettuale" tra legali, informatici, archivisti e coloro che, in qualità di responsabili (interni o esterni all'organizzazione), gestiscono il processo adottato per la conservazione digitale dei documenti.

Un buon contratto di erogazione di servizi di *cloud computing* (e di conservazione digitale dei documenti) dovrà dunque essere il frutto dell'applicazione di norme che regolino la responsabilità civile del fornitore, nonché i processi di sicurezza e di tutela della riservatezza delle informazioni, stabilendo con quali modalità e da chi viene garantita la sicurezza dei dati. Nello stabilire le previsioni contrattuali si dovranno anche tenere presenti tutti gli obblighi

richiamati da discipline specifiche e di settore come, ad esempio, quella che consente la deresponsabilizzazione dei vertici apicali in caso di commissione di reati informatici, attraverso la predisposizione di un idoneo modello organizzativo e l'adozione di specifiche procedure per l'ottimizzazione del servizio, da condividere con il fornitore. Nel contratto si dovrà inoltre tenere in conto e prevedere l'applicazione di norme tecniche internazionali o standard ISO[8].

È possibile inserire all'interno dei contratti clausole finalizzate a garantire gli obblighi di riservatezza, la cui violazione comporta la previsione di penali. Per prevenire accessi abusivi, o comunque non consentiti, è inoltre opportuna la previsione dell'impiego della crittografia per i dati di transito oggetto di trasferimento e il ricorso a sistemi adeguati di autenticazione, in modo tale da assicurare la certezza circa l'identità dei soggetti legittimati all'accesso ai dati e alla ricezione degli stessi. Sempre in tema di flussi di dati trasfrontalieri è possibile fissare le garanzie minime necessarie per attenersi alle prescrizioni della normativa comunitaria.

Tra gli obblighi da porre a carico del fornitore dovrebbe esserci anche quello di consentire la portabilità dei dati e l'interoperabilità dell'infrastruttura con le risorse di calcolo dell'utente.

6.2 – ripartizione dei ruoli tra fornitore e utente

Al fine di individuare eventuali profili di responsabilità del soggetto che gestisce i dati, è necessario chiarire l'esatta qualificazione giuridica del fornitore di un servizio di *cloud computing*. Si è ritenuto che questi, anche laddove mantenga propri margini di autonomia, non debba essere considerato un *controller*, ma un *processor*, ciò, in particolare, ove le modalità di gestione dei dati siano concordate dall'utente e dal fornitore mediante specifiche clausole.

In effetti, il fornitore di servizi svolge un'attività di gestione limitata solo a determinati dati e non possiede generalmente quelle competenze specifiche e adeguate a svolgere un ruolo predominante nel loro trattamento; in capo al fornitore rimane tuttavia un margine, assai ampio, di autonomia e conseguente responsabilità (quale *controller*) rispetto ai dati di traffico inerenti la circolazione delle informazioni, nell'infrastruttura o verso le risorse di calcolo dell'utente.

La ripartizione dei ruoli delle responsabilità tra fornitore e utente non può tuttavia essere stabilita rigidamente; i modelli di *cloud computing* illustrati in precedenza possono infatti essere integrati fra di loro, sia nel caso in cui il fornitore offra un servizio integrato, sia nel

[8] come ad esempio la ISO 27001, in termini di garanzie dall'estero nei contratti stipulati con i terzi.

caso in cui più fornitori concorrano a offrire un servizio completo. Basti pensare, a titolo di esempio, al caso in cui il servizio offerto comporti l'elaborazione e la gestione dei dati (archiviazione, effettuazione di copie, trasmissione di dati a terzi ecc.), nel quale occorre distinguere tra le operazioni di elaborazione dati effettuata direttamente dall'applicazione informatica e quella posta in essere dal gestore, in quanto solo in quest'ultimo caso si potrebbero ravvisare profili di responsabilità di quest'ultimo, restando le altre operazioni riconducibili al fornitore del servizio[9].

Particolare attenzione - con l'individuazione di specifiche garanzie - va posta nel caso in cui il fornitore sia legittimato ad appaltare a terzi parte dei servizi, anche solo la gestione/allocazione delle risorse fisiche su cui risiedono i dati.

6.3 – legge applicabile

La legge applicabile alla fornitura di servizi di *cloud computing* nella pratica è spesso quella del luogo in cui è stabilito il fornitore, ciò in particolare quando l'utente aderisca a servizi già esistenti o predisposti per altri. Ove questi il fornitore sia una società con sede all'interno dell'Unione Europea non si pongono ostacoli, dato che si applica la normativa comunitaria. Tuttavia, la problematica attinente alla normativa applicabile in caso di controversie sorte tra il fornitore del servizio e l'utente può presentarsi in termini più complessi, al verificarsi di situazioni nelle quali il fornitore interagisce con altri soggetti.

In un'infrastruttura di *cloud computing* i dati spesso vengono memorizzati in diversi *data center*, che ben possono trovarsi materialmente in più nazioni; il fornitore del servizio può inoltre ricorrere a terzi per lo scambio di risorse di calcolo (si pensi, ad esempio, al fornitore che non ha a disposizione sufficiente capacità in termini di supporti di memorizzazione e si affida perciò ad altri). Questi scambi tra più soggetti determinano un flusso continuo dei dati, così che non è facile individuare con esattezza il soggetto che li gestisce in un determinato momento, né la loro esatta localizzazione; l'utente si limita ad accedere al servizio e sarà il fornitore a reperire i dati e a riaggregarli. Una pluralità di relazioni negoziali ha inoltre luogo quando – nel caso del SaaS – l'azienda fornitrice metta a disposizione un servizio a sua volta ottenuto da altri fornitori, sempre in modalità *cloud computing*.

Dunque, in considerazione del fatto che diversi soggetti potrebbero intervenire nella gestione dell'infrastruttura, occorre disciplinare l'ipotesi in cui il fornitore si avvalga per il compimento di parte di essi di terzi fornitori non residenti nel territorio dell'Unione Europea.

[9] Con riferimento alla prestazione di servizi on-line si richiamano, per quanto assimilabili, le considerazioni già espresse sub 4.1

Le possibili soluzioni proposte vanno dall'impiego di clausole comunitarie tipo, tra l'utente che usufruisce dei servizi e il sub-fornitore; al mandato rilasciato dall'utente al fornitore, affinché quest'ultimo stipuli da sé accordi con il sub-fornitore; alla previsione di specifici accordi contrattuali tra le parti, che impongano la disciplina nazionale o comunitaria.

La predisposizione del contratto può tuttavia non essere sufficiente a porre l'utente al riparo da rischi, dato che i fornitori possono affidare ad altri operatori alcune attività (ivi comprese la gestione delle risorse fisiche che mantengono i dati) e possono essi stessi essere soggetti a vicende societarie (fusioni o acquisizioni) che portano a cambiamenti rilevanti, quali, ad esempio, la sede legale e, conseguentemente, la disciplina normativa applicabile. In sintesi, anche dopo la stipula di un valido contratto, potrebbe essere difficile per l'utente esigere il rispetto degli obblighi che sono stati disciplinati nel contratto stesso, specie nel caso in cui il fornitore non risieda nel medesimo paese ove risiede il contraente destinatario dei servizi.

7. Il *cloud computing* nelle pubbliche amministrazioni: le indicazioni dell'Europa

7.1 – *cloud computing* e pubblica amministrazione

Il *cloud computing* viene generalmente ritenuto uno strumento importante e di grande utilità per le pubbliche amministrazioni, sia sotto il profilo organizzativo e gestionale – poiché favorisce una *governance* unitaria e un'efficace *cooperazione applicativa* e consente un sostanziale vantaggio in termini di riduzione di costi, aumento di efficienza, flessibilità e velocità di realizzazione dei servizi, agevole manutenzione a distanza e aggiornamento dei sistemi- , sia in quanto può consentire alla pubblica amministrazione di mettere a disposizione una serie di risorse condivise per partecipare allo sviluppo dell'intero sistema paese.

Alcuni ambiti in particolare - che richiedono centri di agglomerazione dei dati e punti di confluenza attraverso cui canalizzare le comunicazioni da e per le amministrazioni - possono prevedere interessanti applicazioni del *cloud computing*. Tra questi si possono individuare: la gestione dei servizi pubblici in mobilità, come la gestione di servizi pubblici locali e dei servizi di trasporto o la concessione di utenze; le attività di manutenzione e monitoraggio di grandi impianti e sistemi distribuiti sul territorio; la telemedicina, per la quale vi è molta domanda da parte sia degli operatori che dell'utenza (si pensi alla possibilità, ad esempio, per il medico di esaminare a distanza gli esami clinici di un paziente); l'amministrazione della giustizia (si pensi alla possibilità di istituire delle sezioni specializzate presso alcune sedi o alla gestione dei rapporti con le diverse Procure della Repubblica) la gestione dei rapporti tra la pubblica amministrazione e alcune utenze specializzate (ad esempio il mondo delle

professioni), che utilizzano sistemi contigui come punti di agglomerazione per predisporre pratiche, documenti e dati da inviare alle amministrazioni.

7.2 – criticità

I temi problematici già trattati in precedenza si pongono con maggior forza nel caso del *cloud computing* per le pubbliche amministrazioni, in considerazione sia del loro ruolo strategico nel sistema-Paese, sia per il fatto che le amministrazioni non trattano solo dati "propri" ma anche (soprattutto) dati inerenti i cittadini (dati personali e non).

Un primo tema problematico riguarda il ***digital divide***. Le infrastrutture di *cloud computing* richiedono la banda larga e la capillare e diffusa accessibilità a internet: diventa dunque essenziale che tutte le amministrazioni siano raggiunte dalla banda larga, per evitare che non possano dialogare tra di loro. Il tema del *digital divide*, finora visto e trattato come un principio di uguaglianza tra i cittadini, diventa un punto fondamentale da superare per lo sviluppo del sistema paese. In quest'ottica occorrerà, a maggior ragione, adottare criteri e regole che assicurino la governabilità fruibilità della banda larga, dato che non possono essere i gestori a decidere le politiche di priorità di instradamento del traffico dati; né si può immaginare d'altra parte il fatto che sulla banda larga si vada semplicemente per ordine di accesso può comportare delle difficoltà pratiche: (sarebbe un problema se la cooperazione applicativa tra amministrazioni pubbliche non deve essere fosse rallentata o bloccata dal traffico generato dagli utenti che scaricano film o brani musicali).

Un secondo tema attiene alla a**deguatezza delle infrastrutture.** È necessario studiare modalità di utilizzo delle infrastrutture di *cloud computing* che siano adattabili alle singole organizzazioni: occorre a tal fine esaminare e comprendere con precisione le esigenze reali delle amministrazioni. In altri termini, l'offerta proposta dai fornitori non deve essere molto al di sopra, né molto al di sotto delle reali necessità delle pubbliche amministrazioni.

Un terzo tema riguarda i**nteroperabilità e portabilità.** Per la pubblica amministrazione l'utilizzo di modelli di *public cloud*, proposti oggi per molti servizi di archiviazione e di posta elettronica, presenta evidenti criticità sotto il profilo della riservatezza dei dati, in particolare con riferimento ai requisiti di sicurezza richiesti per essere conformi alle normative vigenti in tema di trattamento di dati personali e di disponibilità dei servizi. Al contrario, dato che nel settore pubblico vi è l'aggregazione di istanze diverse e provenienti da vari soggetti, la scelta di soluzioni condivise (seguendo il modello dei *private cloud* dedicati a grandi imprese o il modello del *community cloud*) può limitare soluzioni personalizzate che comportano inutili repliche sul territorio, ove sono stati sviluppati applicativi diversi per soddisfare medesime

esigenze[10]. La soluzione scelta dovrebbe consentire all'amministrazione di migrare i servizi da un fornitore a un altro, senza restrizioni tecniche o contrattuali e un eccessivo aumento dei costi. Anche tempi e modalità di resa delle informazioni e della restituzione dei dati devono essere definiti contrattualmente. In sintesi, è di estrema importanza per le amministrazioni pubbliche evitare ogni forma di vincolo inscindibile con il fornitore.

Quarto tema problematico è quello dei r**apporti con il fornitore.** Nella migrazione ai servizi di *cloud computing* le amministrazioni diventano completamente dipendenti dall'adeguatezza della professionalità dei fornitori. Ogni (anche temporanea) inutilizzabilità e/o inefficienza dei servizi può avere un impatto fortemente negativo per i cittadini (basti pensare ai danni che può causare l'inaffidabilità del servizio nell'ambito della sanità) e tradursi non solo in perdite economiche, ma anche in notevoli danni di immagine per le amministrazioni. In quest'ottica è fondamentale introdurre nei contratti clausole che prevedano un risarcimento dei danni, che descrivano, con la massima precisione, le prestazioni che l'amministrazione si attende dal fornitore e che chiariscano come determinate prestazioni siano di cruciale interesse. Ove possibile è opportuno inibire ai fornitori l'appalto a terzi di una parte dei servizi, anche solo la gestione/allocazione delle risorse di calcolo su cui risiedono i dati. In caso contrario occorre prevedere nel contratto specifiche garanzie relativa al sub-appalto. In ogni caso, è opportuno imporre al fornitore di rendere noto all'amministrazione l'affidamento dell'appalto a terzi.

7.3 – le indicazioni dell'Europa

L'Unione Europea ritiene che il *cloud computing* (con i suoi possibili sviluppi) sarà utilizzato da un gran numero di cittadini, piccole e medie imprese e pubbliche amministrazioni dell'Unione e che possa essere un importante strumento di sviluppo anche per quest'ultime. Per tale ragione l'Unione raccomanda ai governi di studiare con attenzione il ruolo che il *cloud computing* potrà giocare nel contesto della protezione delle informazioni e delle infrastrutture, tenendo conto delle peculiarità e delle criticità che esso presenta.

Il contesto dinamico in cui si muove il *cloud computing* comporta cambiamenti di difficile comprensione e una particolare vulnerabilità agli attacchi e difficoltà nei controlli. Ne consegue la necessità per gli amministratori pubblici ad ogni livello - specie nel caso in cui molti servizi siano spostati simultaneamente su un'infrastruttura – di valutare adeguatamente le interconnessioni e l'interdipendenza che caratterizzano un'infrastruttura di *cloud*

[10] Nel settore privato, invece, l'uso dei servizi di *cloud computing* potrebbe fornire benefici alle piccole realtà carenti di fondi sufficienti per accedere a servizi di classe superiore resi più economici dall'erogazione a soggetti aggregati e in modalità di *cloud computing*.

computing, nonché di esaminare con attenzione e singolarmente i requisiti di validità e sicurezza delle soluzioni proposte, comparandoli con i livelli di disponibilità dell'infrastruttura, tenendo conto del fatto che il successo nell'utilizzo di un determinato servizio non comporta automaticamente che sia possibile procedere nello stesso senso con altri servizi.

Ai governi nazionali si suggerisce dunque di studiare e adottare strategie e cautele a lungo termine, che tengano conto delle implicazioni che hanno i modelli proposti di *cloud computing*, per la loro sicurezza e disponibilità, per i prossimi dieci anni, nel contesto dell'economia nazionale e dei servizi ai cittadini. Si suggerisce anche di studiare una strategia volta ad evitare il proliferare di piattaforme e formati di dati incompatibili tra di loro, la trascuratezza e l'inefficienza nella valutazione della sicurezza, la mancanza di una massa critica.

In altri termini, una strategia nazionale per il *cloud computing* deve tendere a comprendere e indirizzare gli effetti di un'interoperabilità e interdipendenza nazionale e sovranazionale, e prevedere e gestire l'impatto di possibili inconvenienti, valutare l'opportunità di introdurre linee guida per i fornitori di servizi di *cloud computing* (simili a quelle già adottate nel settore delle telecomunicazioni) ed essere preparati per eventuali possibili crisi.

In riferimento alla normativa si sottolinea che oltre ai dati sono soggette a normativa diversa (a seconda della legge applicabile e della scelta dei fornitori) anche le applicazioni e i servizi, con particolare riferimento ai modelli di licenza; ragione per cui si suggerisce di privilegiare le soluzioni proposte da coloro che privilegiano soluzioni *open-source*, piuttosto che quelle *close-source*. Inoltre, il *cloud computing* in genere beneficia della globalizzazione economica, per cui i fornitori (e implicitamente gli utenti) si avvalgono di risorse anche umane, nei paesi in cui i costi sono inferiori. Anche sotto questo profilo è opportuno individuare regole che privilegino fornitori che fanno riferimento a paesi nei quali i diritti sono tutelati.

8. Il *cloud computing* nelle pubbliche amministrazioni: l'approccio italiano

8.1 – iniziative

In Italia lo sviluppo del *cloud computing* - come strumento utile per risolvere alcuni tra i più importanti punti critici dei sistemi informativi pubblici - è oggetto di valutazione sin dal 2008. Si fa riferimento, in genere, al paradigma del *cloud computing* da utilizzare nella pubblica amministrazione per indicare: forme grammaticali simili (linguistica); strumenti tecnologici

affini; una filosofia informatica, sinonimo di trasparenza, efficienza ed efficacia amministrativa, di democrazia.[11]

Nel giugno 2012 *DigitPA* ha pubblicato un documento contenente raccomandazioni e proposte sull'utilizzo del *cloud computing*, che ne affronta gli aspetti più rilevanti (sicurezza e privacy; aspetti economici, legali e contrattuali; ricadute per le infrastrutture e i servizi), con l'intento di "fare il punto" sulle considerazioni e proposte della pubblica amministrazione in Italia, ma anche di fornire un supporto concreto alla definizione di politiche e contratti di esternalizzazione della gestione ICT delle pubbliche amministrazioni.

Dal dicembre 2012, con la pubblicazione dell'"Agenda Digitale", le pubbliche amministrazioni nell'acquisizione di programmi informatici possono scegliere di fare ricorso al *cloud computing*; si tratta però di una alternativa ad altre modalità di acquisizione di programmi informatici, che assume parametri di valutazione legati all'acquisto di programmi informatici, più che all'utilizzo di servizi informatici[12].

8.2 - Organizzazione e uniformità

Il panorama delle pubbliche amministrazioni italiane è molto complesso, composto di 30.000 soggetti di diverse dimensioni (anche in termini di utenza servita), incaricate degli stessi servizi e degli stessi compiti istituzionali e di gestione, ma con sistemi di *governance* molto spesso diversi, nonostante gli obblighi di uniformità imposti dalla normativa vigente (ad esempio nel rendere accessibili al cittadino determinati servizi o nell'adozione di piani di continuità operativa e *disaster recovery*).

La ricerca dell'interoperabilità e della standardizzazione all'interno di questo sistema richiede molto tempo e si scontra spesso con le istanza di autonomia degli enti regionali e locali e con la "sindrome del possesso del dato", ciò nonostante il dato sia del cittadino e non della pubblica amministrazione, che deve solo gestirlo per scopi sociali di uso, proteggendolo e tutelandolo. In presenza del processo di federalismo istituzionale e amministrativo in atto, se l'insieme dei sistemi informativi delle amministrazioni - che pure sono tenute al rispetto delle

[11] *DigitPA* ha svolto specifiche attività progettuali e di studio sul tema, attraverso incontri con le aziende, attenzione nei confronti dell'uso del *cloud computing* all'interno delle linee strategiche ICT di alcuni paesi, partecipazione a gruppi di esperti UE e a studi e progetti pilota finanziati dai programmi FP7 e CIP, organizzazione di giornate di studio sull'infrastruttura *cloud computing* e la pubblica amministrazione, istituzione di un gruppo di lavoro denominato "*cloud computing* e pubblica amministrazione".

[12] Ripercorrendo la storia dell'informatica italiana è interessante notare come nel corso di venti anni si sia passati dallo sviluppo esclusivo di programmi da parte della Pubblica Amministrazione (tuttal'più avvalendosi di sviluppatori esterni) previso dalla L. 39/93, all'utilizzo (previo adattamento alle esigenze della singola amministrazione) di programmi sviluppati da e per altri soggetti, previsto dal Codice dell'Amministrazione Digitale,

medesime norme - continuerà a non essere governato in termini di standard dei dati, di progettualità sistemica e di pianificazione nazionale, la tendenza alla differenziazione e alla frammentazione, con conseguente mancanza di interoperabilità, sarà ulteriormente accentuata e aggravata rispetto alla già molto critica situazione attuale.

I modelli di *cloud computing* possono funzionare in questo senso come elementi di catalizzazione, per costringere le pubbliche amministrazioni a seguire la strada dell'industrializzazione e della standardizzazione dei processi per raggiungere l'obiettivo - oramai troppo spesso invocato - di sviluppare in modalità digitale tutte le procedure amministrative. Attraverso il *cloud computing* di fatto si può imporre una standardizzazione, che consente l'omogeneizzazione delle procedure: gli enti omogenei potrebbero infatti avere sistemi informativi funzionalmente equivalenti – se non identici – afferenti ai medesimi procedimenti amministrativi standardizzati, che differiscano solo dal punto di vista dimensionale[13].

Anche dal punto di vista economico il modello del *cloud computing* può avere effetti molto sensibili sul fronte della riduzione dei costi, a condizione di riorganizzare e coordinare i processi. In questo momento, nelle pubbliche amministrazioni le risorse di calcolo sono spesso dimensionate sul livello di massima richiesta; pertanto, la capacità complessiva di calcolo della pubblica amministrazione è pari alla somma dei picchi di fabbisogno di calcolo delle singole amministrazioni, anche se tale capacità non è sempre necessaria dato che le risorse realmente utilizzate sono pari alla somma delle medie dei fabbisogni di calcolo delle singole amministrazioni. I modelli di *cloud computing* possono annullare il sovradimensionamento attraverso la distribuzione dei momenti di picco.

Nella direzione dell'omogeneità conduce sia il Codice dell'Amministrazione Digitale, che la normativa in materia di tutela dei dati personali, che impongono i medesimi obblighi a tutte le amministrazioni pubbliche, senza distinzione (anche ai comuni piccoli e piccolissimi e alle scuole di ogni ordine e grado). La confusione e l'ambiguità di formulazione di alcune norme è tale da renderle inapplicabili e farle disattendere dagli interessati, perché la loro attuazione implicherebbe costi di progettazione e di esercizio non proporzionati alle dimensioni dell'organizzazione e soprattutto competenze tecniche e organizzative difficilmente accessibili a molte amministrazioni[14]; in questo senso, il *cloud computing* potrebbe essere lo

[13] D'altra parte il *cloud computing* costringe alla interoperabilità più di quanto possano fare tutte le indicazioni normative già da tempo previste dal Codice dell'Amministrazione Digitale

[14] Si vedano gli adempimenti previsti dal Codice dell'Amministrazione Digitale in tema di continuità operativa e sicurezza dei dati, dei sistemi e delle infrastrutture delle amministrazioni pubbliche, che in particolare richiedono di redigere un piano di continuità operativa - pur tenendo conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche - e di predisporre un piano di *disaster recovery*, adottato previa redazione di un apposito studio di fattibilità. Si tratta di obblighi difficilmente attuabili dalle piccole amministrazioni locali che, prive di

strumento per permettere a tutti di adeguarsi più facilmente e con costi minori a norme e regole tecniche che altrimenti sarebbero disattese[15].

8.3 - Rapporti con i fornitori e responsabilità dell'amministrazione

Nel considerare l'importanza del rapporto fra l'utente-amministrazione e il fornitore, occorre evidenziare come sia essenziale che i servizi offerti siano "garantiti" da un accreditamento ufficiale che assicuri la conformità ai requisiti normativi, di sicurezza, di qualità del servizio e di responsabilità legale, basati su contratti standard. E' possibile così assicurare alle amministrazioni l'assolvimento degli obblighi di legge o di esigenze politico-strategiche del paese. Come avvenuto nei casi della rete unitaria della Pubblica Amministrazione e del Servizio pubblico di connettività, è opportuno prevedere l'istituzione di un progetto nazionale e sistemico finalizzato a realizzare l'infrastruttura tecnologica del paese che, analogamente a quanto avviene in altri paesi, dovrebbe rispondere a un unico responsabile informatico generale, che abbia adeguati poteri e strutture permanenti di *governance* e di gestione.

Tali cambiamenti dovrebbero essere necessariamente accompagnati da una regolamentazione dei servizi di cui si intende usufruire, attraverso la loro contrattualizzazione; i servizi accessibili attraverso le infrastrutture di *cloud computing*, infatti, possono essere costituiti da un insieme di contratti quali licenza d'uso software (anche se in maniera relativamente limitata), approvvigionamento hardware, outsourcing, hosting, etc. Tale regolamentazione è importante già in relazione ai processi di conservazione digitale dei documenti che le pubbliche amministrazioni stanno avviando, ma acquisirà un'importanza ancora maggiore ove si proceda verso il trasferimento sulle infrastrutture di *cloud computing*.

La gestione di contrattualistiche complesse, tuttavia, richiede un cambiamento per la pubblica amministrazione, che, da un lato, deve avere la capacità di individuare con precisione le esigenze da soddisfare, dall'altro deve disporre di sufficiente conoscenza tecnico-giuridica e avere la capacità di capire cosa succede presso i fornitori[16]. Le modalità con cui redigere e predisporre le condizioni generali di contratto, infatti, dovranno essere il risultato di una

---

adeguate competenze tecniche e organizzative, possono eludere l'obbligo interpretando a loro favore l'inciso già citato.

[15] Su un totale di circa 8.100, circa 7.500 comuni hanno meno di 20.000 abitanti e quasi 6.000 comuni hanno meno di 5.000 abitanti. Le ASL sono circa 400 (il numero varia in continuazione) e le scuole sono circa 14.000. Il costo di adeguamento alle norme non è proporzionato ai parametri dimensionali e molte amministrazioni sono nella pratica impossibilità di rispettare molti adempimenti, anche nei casi in cui le norme rispondono a finalità d'interesse generale per la sicurezza del paese.

[16] L'analisi preliminare delle esigenze da soddisfare è evidentemente determinante anche nella predisposizione dei bandi di gara, finalizzati alla scelta del fornitore.

personalizzazione sullo specifico servizio richiesto, evitando accuratamente contratti frutto di clausole standard, applicate in realtà diverse dalle amministrazioni pubbliche.

9. Dimensione politica del *cloud computing* ed esigenze di armonizzazione

9.1 – *cloud* per le amministrazioni e strategie nazionali

La concentrazione del potere informativo nelle mani dei gestori delle infrastrutture di *cloud computing* può avere una significativa rilevanza strategica, specie se i dati sono quelli trattati da amministrazioni pubbliche. In altri termini, l'uso del *cloud computing* assume un'estrema rilevanza in termini di controllo delle informazioni e delle strategie industriali di un paese. Per le pubbliche amministrazioni, infatti, uno degli obiettivi principali è mantenere la sovranità e il controllo sui dati. Ciò vale anche nel caso di *data base* che non possono definirsi davvero strategici, nonché di *data base* qualificabili come archivi di dati aperti (*open data*). È peraltro evidente che le problematiche attinenti alla sicurezza, alla riservatezza e al controllo dei dati si pongono in modo molto diverso, a seconda della tipologia di dati che vengono trattati.

In mancanza di un'armonizzazione normativa, infatti, le situazioni di fatto che si realizzano con il trasferimento dei dati su un'infrastruttura di *cloud computing* – in particolare la perdita del controllo dei dati da parte dell'amministrazione, che dispone *in loco* esclusivamente di apparati di connessione a internet e stazioni di lavoro - non trova riscontro negli obblighi giuridici che, quanto meno nel contesto italiano, in virtù della normativa vigente, restano in capo ai responsabili dell'amministrazione. Questi ultimi, ad esempio, restano "titolari" del trattamento dei dati personali, anche con riferimento agli obblighi in tema di sicurezza, ciò nonostante la responsabilità di garantire l'integrità e la riservatezza dei dati gravi, di fatto e per contratto, sul fornitore di connettività internet.

Nel momento in cui le strutture che ospitano le infrastrutture di *cloud computing* sono al di fuori della giurisdizione dello Stato, e sono gestite da privati, l'amministrazione è tenuta a considerarne tutte le implicazioni (ivi compresi i rischi connessi con la violazione della sicurezza, della riservatezza, della proprietà intellettuale e industriale). Ancora, ove l'amministrazione si avvalga di un privato per realizzare i servizi in modalità *cloud computing*, la scelta non può che cadere su grandi imprese che dispongono di risorse adeguate, ovvero multinazionali che hanno sede e interessi in altri paesi e rispetto alle quali si pone il tema del trasferimento dei dati all'estero, nonché della possibile influenza che la politica dei paesi di appartenenza può avere anche sulle scelte tecniche adottate.

È ben vero che un soggetto pubblico può imporre al fornitore l'adozione di adeguate misure di sicurezza, nonché di procedure che prevedano la messa a disposizione di dati a condizioni

rigidamente predefinite, si ribadisce – tuttavia – che ci si deve chiedere se e in che misura l'adozione di clausole contrattuali sia sufficiente per dare adeguate garanzie alle amministrazioni conferenti i dati, nel caso in cui nei paesi interessati siano vigenti normative diverse.

9.2 – un *cloud computing* europeo

In alternativa è stata suggerita la creazione di un'infrastruttura tecnologica nazionale che renda disponibili servizi certificati, erogati da soggetti accreditati (eventualmente un raggruppamento di piccole imprese locali), che rispondono dal punto di vista funzionale, tecnico, contrattuale e soprattutto di fiducia, ai requisiti funzionali e normativi prescritti per le amministrazioni [17].

Tuttavia, realizzare un'infrastruttura di *cloud computing* capace di erogare servizi, non è solo complesso per gli aspetti tecnici organizzativi e di *governance*, ma soprattutto per la necessità di rivedere gli strumenti normativi e regolamentari abilitanti o di predisporne di nuovi. Da un lato una dimensione molto ridotta dell'infrastruttura così realizzata potrebbe non consentire il raggiungimento della massa critica necessaria per consentire l'approntamento delle risorse tecniche e delle competenze necessarie per soddisfare le esigenze di sicurezza già evidenziate, a meno di non avere la disponibilità a investire ingenti risorse economiche nella sua realizzazione e gestione. D'altra parte, anche in questo caso, in mancanza di un adeguamento normativo, la previsione di clausole contrattuali che garantiscono l'adempimento degli obblighi da parte del fornitore potrebbe non essere sufficiente.

Per altro verso, l'idea di un'infrastruttura di *cloud computing* "rinchiusa" tra confini nazionali – o ancor più in confini locali – mal si concilia con l'attuale situazione europea, caratterizzata da leggi comuni su aspetti centrali dell'economia e della vita sociale. Basti pensare al fatto che declinare il paradigma di *cloud computing* entro confini nazionali o locali può far sorgere interrogativi in tema di libera competizione all'interno del mercato comunitario.

Appare quindi auspicabile propendere per un modello di *cloud computing* su scala europea, come spazio sovranazionale virtuale, dotato di regole comuni applicabili, sia per quanto riguarda la normativa per le politiche di sicurezza, sia per l'interoperabilità e la definizione di standard tecnici, sia – anche - attraverso il coinvolgimento delle imprese IT europee.

[17] Alcuni servizi critici, ad esempio quelli relativi alla firma digitale, sono già stati affidati a soggetti privati fiduciari che operano in modo conforme al Codice dell'amministrazione digitale e altri se ne potrebbero aggiungere, come ad esempio i servizi di *Identity Management*. Altri servizi, tra cui la gestione del Sistema Pubblico di Connettività, sono affidati all'Agenzia per l'Italia Digitale (già DigitPa)

In primo luogo l'Unione Europea ha una dimensione tale da poter sviluppare il settore IT verso il *cloud computing* senza dover puntare su improvvisate conversioni di imprese operanti in settori affini. In secondo luogo, il ricorso a imprese residenti negli Stati Uniti deve essere ponderato alla luce del quadro normativo locale, che in materia di sicurezza dei dati offre minori garanzie e lascia molto spazio di accesso alle informazioni da parte dei poteri pubblici. Inoltre in ambito europeo è possibile legiferare imponendo norme uniformi agli stati membri. Da non trascurare, infine, il fatto che una soluzione di questa portata potrebbe essere utilizzata anche in un contesto pan-europeo di assistenza per le emergenze.

Le istituzioni europee stanno lavorando nella direzione indicata. La nuova strategia della Commissione europea si propone infatti di accelerare e potenziare l'accesso alla nuvola informatica in tutti i settori economici, mediante alcune azioni chiave volte ad eliminare gli svantaggi costituiti dalla pletora di norme tecniche in uso, a sostenere i sistemi di certificazione a livello europeo destinati a fornitori affidabili di servizi condivisibili nel cloud, elaborare clausole contrattuali tipo (inclusi accordi sul livello dei servizi), creare un partenariato europeo per il cloud che coinvolga gli Stati membri e l'industria, in modo da sfruttare il potere d'acquisto del settore pubblico per orientare il mercato europeo, incrementare la competitività dei provider europei di servizi condivisibili e offrire servizi di e-government migliori e più convenienti.

Riferimenti bibliografici

Dottrina

N. Bottero, *Le nuove prerogative d'autore nell'era di Internet*, Giur. It. 2011, 8-9

A. Mantelero *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo,* in *Dir. Inf.* 2012, p. 135 ss

A. Mantelero, *Data protection e attività di impresa. Verso dove guardano gli USA ?* Dir. informatica 2011, 03, 457

A. Mantelero, *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali e aziendali*, Dir Inf. 2010, 673

Documenti

2012 – European Commission, *Communication from the Commission to the European Parliament, the Council, The European Economic and social Committee and the Committee of the Regions – Unleashing the Potential of Cloud Computing in Europe* (COM(2012)529 final)

2012 – European Commission, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (COM(2012) 11 final)

2012 – DigitPA, *Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione*, ver. 2.0

2012 - Forum PA – Quaderni, *La PA sulla nuvola – G-Cloud: innovare per guadagnare efficienza e ridurre I costi*

2012 - Garante per la protezione dei dati personali, *Cloud Computing: indicazioni per l'utilizzo consapevole dei servizi*

2011 - ENISA, *Priorities for Research on Current and Emerging Network Technologies*

2011 - ENISA, *Seurity & Resiliance in Governmental Clouds - Making an informed decision*

2010 – *Un'agenda digitale per l'Europa*, COM(2012) 245 def/2

2010 – IBM - N. Coleman, M. Borrettt, *Cloud Security, who do you trust?*

2010 - The Aspen Institute – D. Bollier, *The Promise and Peril of Big Data*

2009 - Art. 29 Data Protection Working Party, *Working Document 1/2009 on pre-trial discovery for cross border civil litigation*

2009 - IBM, *Cloud Security Guidance*

2009 - *Open Cloud Manifesto*, www.opencloudmanifesto.org

2009 - Expert Group Report - L. Schubert, *The Future of Cloud Computing. Opportunities for European cloud computing beyond 2010*