JLIS.it
Italian Journal of Library and Information Science
Rivista italiana di biblioteconomia, archivistica e scienza dell'informazione

Cloud computing. Il contesto giuridico e le aziende di fronte ad un fenomeno controverso

Maria Concetta De Vivo

Introduzione

Il cloud computing può essere definito come «l'archiviazione, l'elaborazione e l'uso di dati su computer remoti e il relativo accesso via Internet. In altre parole gli utenti hanno a disposizione una potenza di elaborazione quasi illimitata, non sono tenuti ad investire grandi capitali per soddisfare le proprie esigenze e possono accedere ai loro dati ovunque sia disponibile una connessione Internet».[1]

In Europa sono numerose le iniziative volte a sostenere lo sviluppo della tecnologia cloud, sia da un punto di vista normativo sia finanziario; i punti di sviluppo contenuti nell'Agenda digitale Europea sono mirati in tal senso. Gli obiettivi europei hanno coinvolto

[1] *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico sociale europeo e al Comitato delle Regioni, Sfruttare il potenziale del cloud computing in Europa*,
http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52012DC0529

JLIS.it Vol. 6, n. 2 (May 2015)
DOI: 10.4403/jlis.it-11214

anche il nostro paese che ha provveduto a regolamentare gli sforzi governativi attraverso la compilazione dell'Agenda digitale italiana.

Il fenomeno "cloud" ha origine negli USA e si è successivamente sviluppato in Europa ed in Italia, dove sembra muovere i primi passi. In realtà non rappresenta una assoluta novità nel settore e potrebbe essere considerato come l'evoluzione del c.d. *distributed computing* ("calcolo distribuito", tipica attività di *computer science* che sfrutta le potenzialità di diversi computer) di cui fa parte, a sua volta, il *grid computing* ("griglia" su cui "poggia" il calcolo distribuito). Pertanto si potrebbe definire il *cloud computing* come la "rivoluzionaria" evoluzione del *grid computing*. La novità rivoluzionaria consisterebbe nel modello di *business* che ne è alla base, ossia l'offerta di «*distributed computing*». In realtà, nel mercato tradizionale, il modello è utilizzato da tempo, come nei casi di fornitura e di somministrazione di servizi quali gas, elettricità, telefonia ed altro. L'originalità del *cloud computing* consiste, dunque, nella erogazione di componenti tipiche di un ambiente informatico (dell'*IT*) in cambio di un corrispettivo, permettendo, di fatto, l'utilizzo di tecnologia *web-based*. La tecnologia "basata sul *web*" permette di accedere con facilità alle funzioni offerte grazie ad un normale *web-browser* e cio' consente all'utente di interagire da qualsiasi luogo si trovi.

Cloud e Aziende

Nonostante le caratteristiche vincenti, la tecnologia cloud sembra faccia fatica ad essere accettata, soprattutto dagli utenti finali. In tal senso le statistiche di settore denunciano un panorama piuttosto deludente. Alcune imprese, intervistate sull'adozione di strategie cloud per la propria attività, hanno dimostrato forti perplessità. Il 43% degli intervstati, fra i quali prevalentemente professionisti IT, ha risposto negativamente; mentre solo il 28% ha ammesso di aver intenzione di approntare delle strategie in tal senso (*Cloud Survey 2012: Lo Stato Del Cloud Computing in Italia* 2012). Alla domanda

relativa a quale tipologia cloud si è maggiormente interessati, le risposte hanno evidenziato un'attenzione (48%) verso un cloud di tipo Saas (S*oftware as a service*), seguito dalle tipologie IaaS (*Infrastructure-as-a-Service)* ed infine Paas (*Platform-as-a-Service*). Alla richiesta, rivolta ai dirigenti di impresa e dipendenti di aziende, su come utilizzare il cloud nel proprio ambito lavorativo, le risposte hanno evidenziato un generico intento di "fare business" e di ottimizzare la propria attività. L'aspetto più interessante è emerso dalle risposte alla classica domanda inerente la natura del cloud: più della metà degli intervistati è parsa vaga e confusa. Questo atteggiamento risulta comune sia agli "utilizzatori finali" europei (Italia compresa) sia statunitensi, dove più della metà degli impiegati del governo USA conferma di aver lavorato o di lavorare con tecnologie cloud ma di non comprendere bene in cosa esse, effettivamente, consistano. Probabilmente questa perplessità deriva dal fatto che il target a cui si rivolge il prodotto tecnologico in questione, è rappresentato da imprenditori, cittadini comuni, dirigenti delle pubbliche amministrazioni che sono interessati ad utilizzare la tecnologia solo ed esclusivamente per risolvere i propri problemi e le proprie necessità, piuttosto che a conoscerne le potenzialità tecniche. Il cloud, dunque, mancherebbe della caratteristica di immediatezza e trasparenza, rimanendo confinato nell'ambito dei prodotti pensati "per addetti ai lavori". Tutto ciò in contrasto con una delle principali leggi (non scritte) del marketing che fonda il successo della campagna di presentazione di un prodotto, proprio sulla trasparenza e sulla chiarezza delle sue caratteristiche, in modo da ottenere la piena fiducia dei potenziali clienti.

In ambito privato, nel corso di un rilevamento del 2012 (*Cloud Survey 2012: Lo Stato Del Cloud Computing in Italia* 2012), gli intervistati, alla domanda se si è disposti ad investire nel cloud, hanno risposto in modo incoraggiante, evidenziando, così, come gli investimenti per il cloud computing siano in rialzo. Infatti il 46% ha dichiarato di avere piani di sviluppo del cloud, intendendo investire una somma tra il 5 e il 20% del budget ICT aziendale.

Nel settore pubblico il cloud si colloca al top delle liste delle priorità IT, pur restando forti perplessità in tema di finanziamenti.

Nonostante questa breve analisi poco entusiasmante, emergono almeno due aspetti positivi. Il primo riguarda il contesto lavorativo e l'altro l'ambito energetico ed ambientale.

Il passaggio al cloud comporterebbe nuove opportunità di business (si parla di trecentomila nuovi business, pur restando vago di quale tipo di business si tratti) e produzione di nuovi posti di lavoro (si parla di una cifra compresa tra i trecentomila ed il milione di nuovi posti di lavoro, entro cinque anni). La Commissione europea si propone di "sfruttare il potenziale del cloud computing in Europa" e prevede iniziative intese a realizzare entro il 2020 un guadagno netto di 2,5 milioni di nuovi posti di lavoro in Europa e un aumento annuo del Pil dell'Ue di 160 miliardi di euro (circa l'1%).[2]

La tecnologia cloud ha un impatto anche nel settore del risparmio energetico. Studi di settore (per tutti, Glanz 2012; Scotti 2013) evidenziano alcune curiosità sul consumo dei server utilizzati per la rete e dalla rete. Nel 2012 il consumo è stato di trecento miliardi di watt, una potenza pari alla produzione di trenta centrali nucleari. Inoltre occorre ricordare che i server funzionano 24 ore su 24 e che l'alimentazione elettrica va garantita per l'intero tempo di funzionamento. Le "macchine" consumano e disperdono grandi quantità di calore, ossia di energia, ed è per questo motivo che i locali in cui sono situati debbono essere opportunamente climatizzati, in modo da garantirne l'attività. Emerge, da questo contesto, che l'uso di tecnologia cloud comporterebbe una forte riduzione dei costi, proprio a causa della sua stessa conformazione "architetturale" che, semplificando la gestione delle infrastrutture (*data center*), ne ridurrebbe i consumi (Fasoli 2012). Il cloud rappresenta, inoltre, un contributo risolutivo per l'abbattimento delle emissioni di CO_2

[2] http://www.europarlamento24.eu

dell'ICT ("Tecnologia E Informatica Come Gli Aerei per La CO2 Emessa" 2013).

Sull'inquinamento legato all'IT, occorre aprire una breve parentesi, rinviando eventuali approfondimenti a studi specifici.

Le IT hanno un determinante impatto sulla produzione di CO2. Si prevede che i consumi, entro il 2020, aumenteranno sino al 5-10% del totale della produzione di elettricità globale, come confermano i numerosi studi effettuati da organi competenti.[3] Tutto questo è dovuto all'attività di trasmissione dell'informazione che comporta, necessariamente, un dispendio di energia. È stato appurato[4] che il bit, elemento essenziale per la traduzione in digitale dell'informazione, per essere trasmesso deve essere "commutato in una determinata velocità" e questa operazione necessita di energia. Da monitoraggi effettuati è emerso che la emissione annuale di CO2 dell'uomo è pari a 49 miliardi di tonnellate. Di queste 1 miliardo di tonnellate proviene dal settore dell'IT. Esperti del settore hanno evidenziato che un personal computer emette, nell'arco di 365 giorni, l'equivalente di 1 tonnellata di CO2; un server a sua volta consuma la stessa energia (con conseguente emissione di CO2) prodotta da un SUV che percorre 25 km ("Tecnologia E Informatica Come Gli Aerei per La CO2 Emessa" 2013). L'evoluzione dei processori, progettati per essere sempre più piccoli e sempre più potenti, comporta un aumento di energia "dissipata" e, se un *data center* di medie dimensioni consuma gli stessi kW di un intero quartiere, un grande *data center* utilizzato da grandi aziende, come ad esempio le banche, consuma l'equivalente di energia consumata da una intera città. Secondo ricerche effettuate dal colosso Google, persino una semplice *query* effettuata da un utente della rete, produce piccole emissioni di CO2. Tuttavia sembra inconfutabile che l'inquinamento da IT risulta di minor impatto rispetto a quello di tipo "tradizionale". Ad esempio, è sicuramente maggiore l'inquinamento,

[3] Così il Ceet, Centro per l'efficienza energetica nelle telecomunicazioni dell'Università di Melbourne. Cfr., inoltre, *Environmental Science & Technology*, in http://pubs.acs.org.
[4] IEA http://www.berr.gov.uk

prodotto dall'esigenza di spostamenti da una città ad un'altra in aereo o in macchina, rispetto a quello prodotto da un utente che utilizza tecnologie IT per raggiungere i propri contatti restando comodamente seduto davanti al proprio pc.

L'uso alternativo ed oculato delle IT è dunque un risparmio in quanto "se il 20% dei viaggi di lavoro all'interno dell'Unione Europea fossero rimpiazzati da telecomunicazioni digitali dal 2010 potrebbe essere evitata la produzione di circa 25 milioni di tonnellate di CO2 all'anno"; inoltre, se opportunamente indirizzate e programmate, queste possono ridursi notevolmente impattando nell'ambiente ancor meno dell'1% di oggi.

Occorre ribadire che grazie alla politica di efficienza energetica della *White Economy*, oltre al coinvolgimento di un elevato numero di aziende, si potrebbe generare nuova occupazione ed attraverso lo sviluppo di soluzioni *smart energy*, riferite a contesti urbani nei prossimi anni, gli investimenti crescenti in questo settore produrranno un taglio delle emissioni di gas serra e di CO2 quasi del 70% (Fabbri 2015).

Eni e Facebook sono tra i giganti più virtuosi nel risparmio di energia. L'Eni sta investendo su tecnologie all'avanguardia, mentre Facebook sta optando verso scelte di tipo pratico, come, ad esempio, localizzare i propri *green data center* vicino al circolo polare artico (a Luleå in Svezia), così da poter utilizzare il raffreddamento naturale negli ambienti in cui sono collocati i propri *data center*. In proposito, il consorzio *Green Grid*, insieme all'agenzia EPA,[5] è stato in grado di stimare il valore medio attuale di *Power Usage Effectiveness* (PUE) per i *data center* dislocati in tutto il mondo. Si ricorda che il PUE è lo standard di riferimento per la misurazione dell'efficienza di un *data center* o di un centro di calcolo, in base all'uso che questi fanno dell'energia elettrica. Il valore più basso di PUE registrato fino a oggi sembra appartenere ad un altro colosso dell'IT: Yahoo, forse perché è

[5] http://epanet.ew.eea.europa.eu.

risultata strategica la collocazione dei propri data center nelle vicinanze delle cascate del Niagara.

L'Unione europea intende perseguire entro il 2020 l'obiettivo di ridurre i costi attraverso un'adeguata strategia comune in materia di cloud computing. Bruxelles spera, cioè, che le aziende possano raggiungere un risparmio pari al 30% della loro bolletta informatica, grazie a un maggiore e più razionale uso del cloud.

Sostanzialmente il passaggio al cloud da parte delle aziende, comporterebbe all'incirca un 65% del risparmio energetico.

Per quanto riguarda l'interesse del cloud nel nostro paese, emerge una sostanziale diffidenza da parte delle aziende e questo ci pone negli ultimi posti tra i Paesi europei. Nonostante ciò, il 70% delle aziende si muove verso un consolidamento del valore delle proprie soluzioni IT nell'ottica di migliorare la propria efficienza; fra queste, il 47% considera la componente IT come fondamentale per il successo d'impresa. La percezione di quanto e quale sia lo spazio che le piccole e medie imprese italiane dedicano al cloud computing si deduce dalla consapevolezza che per il 53% di queste, il cloud riveste un ruolo sempre più importante per il successo della propria attività. In realtà questo dato appare più elevato rispetto alla media delle nazioni dell'Europa occidentale, per le quali solo il 33% delle aziende identifica il cloud come una risorsa fondamentale per il successo futuro. È bene ricordare che le piccole e medie imprese intervistate sono prevalentemente aziende giovani, nelle quali è presente almeno un addetto alle IT, con la conseguenza che vi è una maggiore predisposizione al mondo cloud {interessante la lettura di Corsini, Le piccole medie aziende italiane guardano al cloud computing, http://www.businessmagazine.it}.

Si rivelano molto interessanti le opinioni dei professionisti IT italiani (sviluppatori, sistemisti, blogger, web designer, ecc.) sulla tecnologia cloud (*Cloud Survey 2012: Lo Stato Del Cloud Computing in Italia* 2012). Dal sondaggio emerge che il 70% degli intervistati ritiene

determinante la nazionalità italiana del provider e, tra questi, il 30% è disposto ad acquistare soluzioni cloud, ma soltanto da server che risiedano in territorio nazionale .

Una caratteristica vincente del cloud riguarda l'invisibilità delle infrastrutture. Questo aspetto può essere positivo nel caso in cui l'utente le usi in modo immediato e *friendly*, ma può risultare negativo laddove l'invisibilità rappresenti una sorta di opacità nei confronti dell'utente e sorgano delle controversie in riferimento alla ubicazione ed alla gestione delle infrastrutture stesse.

Il cloud comporta, comunque, una serie di vantaggi che spaziano dalla potenza di elaborazione illimitata, al risparmio di investimento di capitali per le proprie esigenze, all' accesso dati illimitato (tramite una connessione internet).

Resta, dunque, la perplessità sul motivo di questa sostanziale diffidenza da parte degli utenti. Diffidenza che forse risale agli aspetti problematici inerenti la sicurezza, la privacy, la connettività. Tutte barriere che, di fatto, ostacolano l'adozione di strategie cloud. Ognuno di questi aspetti comporta, inoltre, risvolti giuridici volti a tutelare l'utente.

Problematiche relative a costi, controllo dati, sicurezza dati, responsabilità, localizzazione dei dati e dei servizi.

Il problema legato al controllo dei dati si rivela determinante nell'analisi del cloud computing.

La compromissione del controllo dei dati può consistere sia in una «perdita» per affidamento a terzi sia nel danneggiamento vero e proprio. Un aspetto, quest'ultimo, maggiormente legato alla sicurezza dei dati. Per perdita si intende lo spossessamento dei dati, laddove vi sia l'inevitabile passaggio di questi dalla sfera dell'interessato a terzi.

Altro aspetto, legato alla perdita dei dati, è quello derivante dalla nebulosità del contesto che spesso non si conosce a sufficienza, in quanto gestito da terzi che utilizzano ambienti "evanescenti" e poco definiti. Ma l'aspetto più emblematico è quello inerente i rischi di violazione costante, e spesso subdola, della privacy che a sua volta può consistere in una duplicazione o nella vera e propria sottrazione dei dati personali.

Tutto ciò determina l'esigenza, da parte dell'utente, di un'adeguata tutela nella operazione di fruizione di servizi cloud, anche attraverso la previsione di un'apposita informativa. Questa dovrà consistere in una chiara conoscenza delle condizioni di spostamento dei dati, così che l'interessato, o il titolare, possano prontamente rientrarne in possesso oppure possano effettuarne la migrazione in altro sistema (*cloud lock-in*).

Il diritto deve, sostanzialmente, soddisfare il difficile compito di assicurare una totale trasparenza sull'operazione inerente il passaggio dei dati. Deve, cioè, imporre chiarezza su tutte le operazioni che riguardano i dati, sia che restino in gestione del soggetto che li possiede sia che "passino di mano", ossia vengano trasferiti al soggetto fornitore di cloud, così da determinare le eventuali responsabilità.

Il cloud comporta una serie di mutamenti che coinvolgono gli stessi utenti. La principale evoluzione è quella inerente il passaggio dal concetto di "cittadini" digitali a quello di "consumatori" digitali, segnando una trasformazione essenziale del ruolo dell'utente che non è più attore, e dunque portatore di specifici interessi sociali, ma diventa un soggetto coinvolto nel contesto consumistico di mercato. Il consumatore, peraltro, è tutelato, dal nostro diritto, in modo attento e completo e la tutela riguarda sia la perdita sia il danno inerente i propri dati.

L'ambiente cloud comporta l'allentamento o comunque il rischio di una perdita di controllo sui dati, in quanto, di fatto, vengono affidati

a terzi. Tali rischi concretizzano le "classiche" forme di violazione della privacy, con particolare riferimento alla sottrazione dei dati o alla loro duplicazione non autorizzata. L' esigenza fondamentale, dunque, nelle tecnologie cloud, è quella di garantire la tutela delle operazioni inerenti la fruizione dei servizi.

Gli interventi pensati in tal senso, sia a livello europeo sia nazionale, sono numerosi e rivolti ad arginare, in tutti i modi, la estrema facilità di utilizzo illecito di dati (duplicazione e/o sottrazione). L'ultima operazione è stata attuata dal gruppo di lavoro Article 29, istituito in ottemperanza a quanto contenuto nella Direttiva 95/46/EC, riunitosi nel settembre del 2014 per discutere di una adeguata normativa in grado di tutelare gli utenti della rete da fenomeni emergenti, come l'Internet delle cose (IoT). L'incontro ha prodotto una interessante analisi pubblicata nel Parere n. 8 del 2014.[6]

La *European Network and Information Security Agency* (ENISA) ha recentemente pubblicato un'analisi sui criteri utili a garantire sicurezza e "resilienza" dei sistemi di *cloud computing* {cfr. Comunicazione della Commissione al parlamento Europeo, "Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale" in eur-lex.europa.eu}. Questi studi rientrano in un quadro di iniziative inerenti la «Cyber Europe 2012».

Anche l'Agenzia per l'Italia Digitale ha analizzato il fenomeno cloud computing emanando una serie di raccomandazioni e proposte sull'utilizzo del cloud computing nella pubblica amministrazione.[7]

In genere, quando si parla di sicurezza ed integrità dei dati, si intende parlare di probabili errori di gestione, incidenti, oppure di veri e propri attacchi in grado di compromettere l'integrità del dato residente nel cloud. In questo caso, al fine di non compromettere la disponibilità dei dati, prima di "affidarli" ad altri, sarebbe opportuno approntare una serie di misure di sicurezza che il nostro ordinamento

[6] http://ec.europa.eu/justice.

[7] http://archivio.digitpa.gov.it/cloud-computing-pubblica-amministrazione.

giuridico prevede e definisce come misure minime di sicurezza. Come ad esempio la regolare copia di backup dei propri dati.

Un diverso approccio nei confronti del trattamento dei dati potrebbe risultare vincente, laddove si optasse per un tipo di protezione che prenda in considerazione la fase di accesso "ai" dati piuttosto che quella di protezione "dei" dati. Questo implica una maggiore attenzione all' identificazione dei soggetti che accedono ai dati. Di conseguenza, oggetto delle procedure di sicurezza non saranno più soltanto i dati, bensì i soggetti che con quei dati avranno a che fare di volta in volta, fermo restando che la procedura di "identificazione" non deve intralciare l'immediatezza della fruizione del servizio da parte dell'utente. Pertanto, una ulteriore forma di garanzia sui dati può essere assicurata dalla previsione di "semplici" forme di verifica e di certificazione dei fornitori di servizi.

In questo contesto operativo, appare evidente quanto acquisti importanza la reputazione del cloud provider, ossia la sua totale affidabilità, anche e soprattutto in riferimento ai parametri inerenti la confidenzialità con il proprio interlocutore (cliente).

Il fornitore cloud deve, cioè, assicurare al potenziale cliente non solo gli elementi standard di sicurezza del dato, peraltro dovuti *ex lege*, ma anche e soprattutto il fatto che, onde colmare la evanescenza dell'ambiente in cui ci si trova ad operare, sarà lui personalmente e concretamente a rispondere di tutto ciò di cui avrà bisogno il proprio cliente. Non solo nella fase di normale gestione ed erogazione ma anche e soprattutto in quella di una eventuale "patologia" del servizio, qualora l cliente decida di migrare o di reagire ad una intrusione, manomissione oppure perdita dei propri dati. In tal senso appare utile la previsione della costituzione di una organizzazione adeguata, come ad esempio il "SOC", *Security Operations Center* {le competenze del SOC rientrano nell'ambito delle attività di monitoraggio dell'*information security*, per il consolidamento nei confronti della gestione degli incidenti di sicurezza informatica, che nel 2012 si è ulteriormente sviluppato, in seguito agli obblighi previsti dagli

standard internazionali quali l'ISO27001 e in particolare l'ISO27035} con il compito di controllare l'infrastruttura relativa alla sicurezza, anche attraverso l'attività di monitoraggio e supervisione dei dispositivi che forniscono protezione all'organizzazione. Un tale sistema avrebbe come scopo la prevenzione e la gestione efficace degli incidenti relativi alla sicurezza.

Breve quadro normativo

Sono numerose, ed in costante aggiornamento, le normative che riguardano la sicurezza dei dati, sia a livello nazionale sia internazionale.

Tra le normative emanate si ricorda la legge 18 marzo 2008 n. 48, con la quale l'Italia ha ratificato la Convenzione del Consiglio d'Europa sulla criminalità informatica firmata a Budapest il 23 novembre 2001; oltre alle normative di settore quali il d.lgs. 196 del 2003, spec. l' All. B (Disciplinare Tecnico misure minime di sicurezza) ed il d.lgs. 28 maggio 2012 n. 69 di modifica al codice, oltre al d. lgs. 6 dicembre 2011 n. 201, c.d. "Salva Italia".

In materia di cloud ci sono stati interessanti interventi anche da parte del Garante italiano, di seguito se ne riportano alcuni, tra i più significativi.

Il Vademecum del Garante della Privacy (del 2012) sintetizza alcune "buone prassi" da rispettare: "Non dimenticare, mai, le responsabilità, in materia di protezione dei dati personali, che permangono in carico all'utilizzatore dei servizi cloud nonostante egli non abbia più la disponibilità, in locale, dei suddetti dati;

- Valutare, nel modo più coscienzioso, previdente e attento possibile, la serietà e l'affidabilità dei vari service provider, prima di aderire ad un qualsiasi programma di gestione in remoto dei dati informatici;

- Informarsi, nel modo più dettagliato possibile, in merito alla legislazione riguardante il trattamento, la tutela e la permanenza dei dati personali ed informatici della nazione in cui risiedono i server; Leggere e rileggere attentamente ogni clausola del contratto che si andrà a stipulare con il provider prescelto;

- Attivare specifici corsi di formazione rivolti al personale addetto alla gestione del patrimonio informatico".

Il Parere del Garante del 4 luglio 2013 riprende quanto affermato nelle "Linee-guida per il Disaster Recovery delle pubbliche amministrazioni"[8] e ricorda, al punto 3.4, dedicato ai servizi cloud, che il fornitore deve indicare "con apposita dichiarazione resa in sede contrattuale, l'esatta localizzazione, o le esatte localizzazioni dei dati gestiti". Grazie a ciò è possibile, per il titolare del trattamento, valutare la corrispondenza del servizio offerto alla normativa in materia di protezione dei dati personali, specialmente in riferimento all'articolo 45 del d. lgs. 196 del 2003. Nelle "Linee-guida per il Disaster Recovery delle pubbliche amministrazioni" al § 6.5 è, inoltre, prevista la possibilità di stipulare contratti ad hoc con la previsione di clausole specifiche, elaborate dalla Commissione Europea nei contratti di fornitura del servizio. Le predette clausole, effettive dal 15 maggio 2010, trasferiscono parte delle responsabilità sul trattamento dati a chi effettivamente li tratta. Considerato che l'attività di *outsourcing* può essere subappaltata anche più volte, nell'ambito del medesimo servizio, deve comunque essere garantita chiarezza su chi sia il responsabile per la sicurezza dei dati. Sul contratto di *outsourcing* si rinvia a studi di settore (Tosi 2001; Dassi 2004; Ricciardi 2000; Caroli and Valentino 2011; Cardarelli 1993; Mantelero 2012).

Il quadro normativo volto a regolamentare il fenomeno del cloud si arricchisce delle dichiarazioni della serie ISO/IEC 2700 sulla sicurezza delle informazioni. Tra queste, la dichiarazione ISO/IEC 27002, sezione 6.2, "*External Parties*", indica come "(…) la sicurezza delle

[8] http://www.agid.gov.it/sites/default/files/linee_guida/linee-guida-dr.pdf

informazioni nell'ambito di una organizzazione non deve essere mai ridotta dall'introduzione di servizi e prodotti di terze parti". Le ISO/IEC 2700 riguardano la sicurezza delle informazioni che debbono sempre essere garantite, in riferimento alla riservatezza, integrità e disponibilità.

Per quanto riguarda le Misure minime di sicurezza, non è possibile, in questo contesto, analizzarle in modo approfondito, tuttavia ci si può limitare a ricordare come il legislatore abbia inteso considerarle "*Misure che riducono al minimo i rischi di distruzione o perdita, intercettazione e manipolazione dei dati personali*" (art. 31 seconda parte Codice privacy). Tali strumenti hanno lo scopo di assicurare l'integrità dei dati oltre che il buon esito e la correttezza del loro trattamento. Quel "minimo" imposto dal legislatore sta ad indicare la necessità del rispetto di un minimo livello di sicurezza, oltre il quale non si può scendere se non si vuole incorrere in pesanti sanzioni. Più specificamente, le misure che debbono essere adottate devono riguardare determinate attività informatiche, quali: la fase dell'autenticazione; la fase delle copie di sicurezza; la protezione da accessi indesiderati (Internet); la protezione da programmi non autorizzati (Virus) e l'aggiornamento tecnologico (tutte misure contenute nel Disciplinare Tecnico Allegato B al d. lgs. 196 del 2003).

Nel complesso il d. lgs. 196 del 2003 sulla privacy può essere considerato un buon testo normativo in grado di regolamentare il settore. Il Codice sostanzialmente delinea sia gli obblighi sia i soggetti obbligati, indicando, oltre alla predisposizione delle misure minime di sicurezza, "chi" deve eseguire la raccolta ed il trattamento (identificazione dei soggetti) e "cosa" si deve fare per rispettare una prassi corretta in tal senso (obblighi di informativa/consenso nei confronti dell'interessato, ecc.). Nel testo normativo è indicata anche la possibilità di nominare dei responsabili del trattamento che, grazie alla loro professionalità, siano in grado di affiancare adeguatamente il titolare nella delicata fase della gestione delle informazioni, per cui, in tal caso, l'obbligo "della sicurezza dei dati" sarà ripartita tra il titolare

(*ex* art. 28, gravato dalla ulteriore responsabilità per *culpa in vigilando e culpa in eligendo*), il responsabile (*ex* art. 29) e gli incaricati (*ex* art. 30)
.

La responsabilità in ambiente cloud si sviluppa in riferimento ai diversi tipi di tecnologia utilizzata, così, ad esempio, nel modello IaaS, il provider del servizio avrà la responsabilità della sicurezza dell'infrastruttura sottostante mentre resterà in capo all'utente/cliente la responsabilità inerente ai sistemi operativi ed alle applicazioni che riguardano l'ottimizzazione dell'infrastruttura.

Nel tentativo di delineare una filiera di responsabilità e definire in capo a chi farle risalire, si potrebbe identificare il titolare del trattamento dei dati nell'utilizzatore dei servizi di cloud computing, con la conseguenza che sarà questo a verificare l'idoneità e l'affidabilità dei fornitori dei servizi di cloud computing. I fornitori di servizi potranno essere equiparati alla figura del tradizionale "responsabile" del trattamento dati, in quanto ad essi, di fatto, è affidato il trattamento stesso.

Un altro aspetto rilevante in ambiente cloud è quello relativo alla la c.d. localizzazione (o anche territorialità) dei dati. L'aspetto è interessante soprattutto in caso di possibili controversie. Rientra in questa ipotesi il difficile compito a cui spesso sono chiamati la polizia e gli organi giudiziari qualora sorga l'esigenza di conoscere, in caso di indagine, il luogo esatto in cui i file di *log* vengono custoditi e le modalità di custodia, al fine di valutare il livello di protezione degli stessi da possibili manomissioni, anche in considerazione della necessità di un immediato accesso ad essi.

L'Europa è da sempre attenta alle tematiche dell'IT, soprattutto al settore dei dati ed al loro sviluppo. Nel 2014, ad esempio, la Commissione europea insieme all'industria europea dei dati si sono impegnati ad investire oltre 2 miliardi di euro in un partenariato pubblico-privato (c.d. *PPP*) in grado di rafforzare il settore. Sullo sviluppo di una "economia dei dati" in Europa si rinvia alla lettura

del Comunicato stampa del 2 luglio 2014 della Commissione Europea ed al MEMO/14/455.

Dall'Unione Europea sono state intraprese numerose iniziative inerenti la possibilità di istituire regole giuridiche comuni da applicare allo specifico fenomeno del cloud computing. Le analisi e gli studi hanno coinvolto 13 paesi europei (tra cui l'Italia) ed hanno riguardato le normative previste per la protezione dei dati.

Il progetto CloudWATCH,[9] sostenuto dalla Commissione Europea, ha costituito un osservatorio sul cloud computing in grado di identificare e promuovere profili standard, *best practices* e linee guida su questo complesso fenomeno tecnologico. Il progetto dovrebbe provvedere anche alla formazione di un Portale web in cui verranno pubblicati i risultati delle ricerche e gli sviluppi del progetto stesso, e verrà dato ampio spazio a utili contenuti (anche di natura giuridica) indirizzati a fornitori e utenti di servizi cloud di tutta Europa.

«Europa 2020 per una crescita intelligente, sostenibile e inclusiva» è un altro studio interessante che risale al 2010, proposto dalla Commissione europea con l'obiettivo di ottenere entro il 2020 il raggiungimento di un uso sociale della tecnologia, la realizzazione delle reti di nuova generazione e l'alfabetizzazione digitale. Il progetto è sviluppato in quattro punti tra i quali è presente anche quello inerente il cloud computing.

Il Regolamento Ue, tanto atteso, dovrebbe giungere alla conclusione dell'attività di negoziato del Consiglio Ue entro il 2015, così da poter giungere a piena operatività entro il 2020. Il condizionale è d'obbligo perché dopo i fatti del Datagate 2013, la procedura di emanazione del provvedimento sembra rallentato, soprattutto a causa degli indiretti interventi delle aziende Usa che tentano di "mitigarne" la portata. È bene ricordare che il provvedimento ha avuto origine nell'ormai lontano 2012 e che il sistema legislativo europeo prevede che il potere di legiferare sia esercitato dal Parlamento (che rappresenta i cittadini

[9] http://www.cloudwatchhub.eu

dell'Unione europea), dal Consiglio (che rappresenta i Governi dei singoli Stati membri dell'Ue) e dalla Commissione. "In linea di principio, la Commissione propone i nuovi atti legislativi, che il Parlamento europeo e il Consiglio devono adottare. La Commissione e i paesi membri applicano poi le norme, e la Commissione si assicura che vengano applicate e fatte rispettare correttamente" (estratto dal sito europeo). Questo sistema, di fatto, impone che i due organi (Parlamento e Consiglio Ue) siano d'accordo nella emanazione degli atti normativi e che questi non possono essere operativi senza l'approvazione di entrambi. Pertanto, se da un lato il Parlamento europeo è stato relativamente veloce nell'emanare il regolamento, la fase di rallentamento sembra derivare dalla difficoltà del Consiglio di raggiungere maggioranze qualificate.

L'Europa sta cercando di concretizzare a tutti i costi una complessa tutela della privacy dei propri cittadini, sviluppando interventi che rafforzino principi già conosciuti o introducano e sviluppino principi nuovi o semi-nuovi, come il diritto all'oblio, ed il diritto a rendere silenzioso il chip (consistente nella possibilità di interrompere in ogni momento il trasferimento dei propri dati ad altri soggetti). Appare controverso e poco chiaro il principio del *Do not track* che riprende la soluzione tecnologica consistente nell'uso di un *header* del tipo *X-No-Track: user-opt-out=explicit* all'interno di ogni richiesta del browser, così da impedire il tracciamento occulto dei consumatori. Il *Do not track* permette, di fatto, all'utente di segnalare a ciascun sito visitato, la sua volontà di essere o meno tracciato nel corso della navigazione e rafforza il principio del consenso informato.

L'Ue, attraverso i suoi interventi, intende, dunque, creare un'unica legge per tutti gli Stati membri, con regole comuni sulla privacy e con identiche tutele sui dati dei cittadini europei coinvolti nei servizi di cloud. A tal fine, si cerca di controllare attentamente la "trasmigrazione" dei dati informativi dai server presenti in Europa e, qualora ciò avvenga, predisporre un trasferimento degli stessi nel

rispetto di "rigide" regole normative, sostanzialmente tutte europee, poste a tutela della privacy.

Nel Regolamento Ue sono stati fissati anche dei limiti al cosiddetto *profiling*, l'analisi della situazione economica, professionale, sanitaria e sociale di una persona. Tra i tanti punti chiave del provvedimento in oggetto se ne indicano solo alcuni. Il *privacy impact assessment* (valutazioni preventive di impatto sulla tutela dei dati) in caso di trattamenti rischiosi; l'obbligo per le aziende con più di 250 dipendenti e per gli enti pubblici di nominare un *data protection officer* ossia un professionista responsabile della protezione dei dati personali; il diritto alla portabilità dei dati da un provider a un altro, in formato neutro; la previsione delle figure dei "*joint controllers*" (titolari congiunti) che potranno "spartirsi" le responsabilità; la previsione del concetto di "stabilimento principale" del titolare, per evitare che un'impresa attiva in più Stati Ue debba fronteggiare gli adempimenti nazionali di ogni singolo Stato; la previsione del ruolo di "*lead authority*", in modo tale che vi sia un solo Garante di volta in volta responsabile dei procedimenti multi-Stato; la previsione di sanzioni fino al 2% del volume d'affari globale di un'impresa, volte a sensibilizzare sulla privacy anche i consigli di amministrazione di grandi colossi multinazionali; l'introduzione del principio della cosiddetta "*accountability*" ed infine il diritto all'oblio, per cui ogni interessato potrà richiedere la rimozione di propri dati personali per motivi legittimi. In realtà questo diritto, tanto atteso e tanto osannato, sembra che, con il passare del tempo, abbia perso la sua caratteristica di novità e si stia trasformando in una sorta di semplice diritto di rettifica. Ben diverso, dunque, dall'originaria versione del provvedimento del 2012.

Dall'impostazione emerge un generale obbligo per le aziende di realizzare un vero modello organizzativo per la protezione dei dati personali.

Cloud e contratto

Il ruolo dei contratti nella regolamentazione delle attività di cloud è determinante. Il contratto, infatti è lo strumento che più si presta alla principale funzione di regolamentare sia la fase pre e inter-contrattuale sia la fase post-contrattuale, soprattutto in caso di patologia del rapporto, prevedendo e regolamentando le ipotesi di inadempimento-risoluzione e reimmisione dei dati in mano al titolare/Interessato. Attraverso di esso e grazie alla presenza delle apposite clausole si intende, di fatto, perseguire una maggiore severità sulle responsabilità al fine di generare fiducia nell'utente finale.

La stessa Ue ha previsto una sorta di *task force* che dovrà controllare i contratti cloud e dovrà predisporre regole e garanzie nei rapporti tra clienti e fornitori. L'intento è di creare condizioni contrattuali sempre più affidabili ed eque per l'utilizzo dei servizi di cloud computing, incrementare la fiducia ed agevolare la stipula di accordi. La *task* sarà composta da esperti, fornitori, consumatori, esponenti del mondo accademico e giuristi, e "lavorerà alla definizione di clausole contrattuali che, per il momento, saranno suggerite su base facoltativa con la prospettiva, in seguito, dopo le necessarie verifiche di diventare obblighi di legge". Il gruppo è il risultato della strategia europea volta a "Sfruttare il potenziale del cloud computing in Europa 27 settembre 2012, volta ad incrementare il ricorso alla "nuvola" in tutti i settori economici. La task di esperti dovrebbe rappresentare un elemento chiave di questa strategia in grado di soddisfare gli sforzi della Commissione di promuovere il mercato unico digitale, infatti ha il compito di aiutare la Commissione a valutare le opzioni disponibili per migliorare il quadro giuridico dei contratti relativi ai servizi clou, previsti sia per i consumatori sia per le piccole e medie imprese" (*Corriere Comunicazioni* 2013). Lo scopo finale dell'Ue è di concretizzare un diritto comune europeo della vendita.

Nel contratto di cloud sarà, pertanto, opportuno inserire una serie di ipotesi, regolamentazioni e clausole a partire dalla clausola risolutiva espressa (*ex* art. 1456 c.c.), attraverso la quale l'utente/consumatore, in

qualità di parte non inadempiente, dichiara la sua intenzione di risolvere il contratto (le cause potrebbero essere: una prolungata interruzione del servizio, oppure gravi e ripetute carenze nei livelli di qualità che il fornitore si è obbligato, invece, a rispettare); il principio di "conservazione del contratto" *ex* art. 1367 c.c. (Cataudella 2009), per cui "certi inadempimenti", non irreparabili, potrebbero essere ridimensionati con soddisfazione di tutte le parti, prima di procedere alla risoluzione contrattuale; dichiarazioni e forme di garanzie e limitazioni di responsabilità, politiche di utilizzo e condizioni di servizio (con rinvio o sviluppo degli *SLA*); ipotesi di filiere di responsabilità ed, infine, l'obbligo del fornitore (in caso di risoluzione del contratto) a prestare tutta l'assistenza necessaria per il passaggio ad un altro fornitore, stabilendo se possibile, in anticipo, con chiarezza, cosa si intende per "assistenza necessaria".

Alle parti è data libertà di regolamentare i rapporti che pongono in essere, anche in riferimento alla contrattualistica internazionale e nel rispetto del c.d. *pactum de lege utenda.* Il contratto di cloud computing dovrebbe rispettare una struttura in grado di caratterizzarlo, concretizzando una ipotesi di "tipicità sociale", idonea a descrivere in maniera inequivoca un modello contrattuale ed in grado di giungere ad una tipicità legale (Sacco 1986, che parla di tipicità "social-giurisprudenziale"; Roppo 1989). La sua struttura dovrebbe assicurare la presenza di una sezione di "*terms of service*", ossia un regolamento in grado di prevedere i rapporti tra *cloud provider* e cliente; un'altra sezione di "*Service Level Agreements*" (*SLA*), rivolta alla sicurezza ed alla previsione di qualità/quantità servizi, di danni, di responsabilità/risarcimento, ed infine una sezione di "*Policy*" *(PLA)*, suddivisa in una parte generale, inerente tutto ciò che è permesso e non è permesso fare nell'intento di arginare gli illeciti; ed in una parte speciale, riservata alla *privacy* ed al trattamento dei dati.

In conclusione, stante la complessità del fenomeno del *cloud computing* e vista l'assenza di una definita disciplina legale, si avverte l'esigenza di predisporre un contratto le cui clausole chiariscano, per quanto

possibile, la posizione assunta dal fornitore, descrivendone la prestazione dovuta e, conseguentemente, le responsabilità.

References

Cardarelli, F. 1993. "La Cooperazione Fra Imprese Nella Gestione Di Risorse Informatiche: Aspetti Giuridici Del C.d. Outsourcing." *Dir. Informaz. Informat.* I: 85 ss.

Caroli, Matteo, and Alfredo Valentino. 2011. "La Strategia Di «outsourcing»." *Analisi Giuridica dell'Economia* 10 (2): 255–72.

Cataudella, Antonino. 2009. *I Contratti. Parte Generale*. Torino: Giappichelli. http://www.ibs.it/code/9788834897188/cataudella-antonino/contratti-parte-generale.html.

Cloud Survey 2012: Lo Stato Del Cloud Computing in Italia. 2012. Milano: Enter. http://www.enterthecloud.it/wp-content/uploads/2012/05/cloud_survey_20121.pdf.

Corriere Comunicazioni. 2013. "Cloud, La Ue Battezza La Task Force per I 'Contratti Sicuri,'" October 28.

Dassi, Anna. 2004. *I Contratti Di Outsourcing*. Milano: Ipsoa. http://www.ibs.it/code/9788821720109/dassi-anna/contratti-outsourcing.html.

Fabbri, Flavio. 2015. "L'efficienza Energetica Italiana Varrà 43 Mld Di Euro Nel 2020." *Key4biz*. Accessed May 6. http://www.key4biz.it/efficienza-energetica-mercato-italiano-43-miliardi-euro-nel-2020/102008/.

Fasoli, Claudio. 2012. "Cloud Computing E Risparmio Energetico." *Data Manager Online*. April 30. http://www.datamanager.it/rivista/approfondimenti/cloud-computing-e-risparmio-energetico.

Glanz, James. 2012. "Data Centers Waste Vast Amounts of Energy, Belying Industry Image." *The New York Times*, September 22. http://www.nytimes.com/2012/09/23/technology/data-centers-waste-vast-amounts-of-energy-belying-industry-image.html.

Mantelero, Alessandro. 2012. "Il Contratto per L'Erogazione Alle Imprese Di Servizi Di Cloud Computing (Cloud Computing Contracts: B2B)." *Contratto E Impresa*, no. 4-5: 1216–22.

Ricciardi, Antonio. 2000. *L'outsourcing strategico. Modalità operative, tecniche di controllo ed effetti sugli equilibri di gestione*. FrancoAngeli.

Roppo, V. 1989. "Contratto." *Dig. Disc. Priv., Sez. Civ.* Torino: UTET.

Sacco, R. 1986. "Autonomia Contrattuale E Tipi." *Rivista Trimestrale Di Diritto Processuale Civile*, 785 ss.

Scotti, Marco. 2013. "Il Consumo Dei Server E Il cloudInternet, Device E I Nuovi Business." *Affaritaliani.it*, January 31. http://www.affaritaliani.it/fattieconti/il-consumo-dei-server310113.html.

"Tecnologia E Informatica Come Gli Aerei per La CO2 Emessa." 2013. *Corriere Della Sera*. January 3. http://www.corriere.it/scienze_e_tecnologie/13_gennaio_04/informatica-tecnologia-emissioni-aviazione_11bfa306-559c-11e2-8f89-e98d49fa0bf1.shtml.

Tosi, Federico. 2001. *Il contratto di outsourcing di sistema informatico*. Milano: Giuffrè.

Maria Concetta De Vivo. Scuola di Scienze e Tecnologie, Università degli studi di Camerino. concetta.devivo@unicam.it

De Vivo, Maria Concetta. "Cloud computing. Il contesto giuridico e le aziende di fronte ad un fenomeno controverso". *JLIS.it*. Vol. 6, n. 2 (Maggio/May 2014): Art: #11214. DOI: 10.4403/jlis.it-11214.

ABSTRACT: In this paper we analyze the cloud computing. The topics covered in the paper include: privacy, industry statistics, cloud and enterprise, data retention, data location, responsibilities in data processing. The European and national legislation and the contract are analyzed in this paper.

KEYWORDS: cloud computing, data protection, contract/agreement, data security, consumers, business.

Submitted: 2014-04-15

Accepted: 2015-03-22

Published: 2015-05-15