Il Sole 24 ORE



5 gennaio 2011

# La protezione dei dati personali al tempo del Cloud Computing

di Massimiliano Pappalardo

Il cloud computingè, nelle più recenti analisi, considerato un tema prioritario dell'agenda di molte imprese. Il processo di esternalizzazione di attività non core – sviluppatosi nello scorso decennio attraverso il ricorso sempre più frequente all'outsourcing - con il cloud giunge alla sua fase più estrema. Saranno, infatti, le banche dati aziendali a poter lasciare i locali dell'impresa per essere ospitate presso reti di data center gestite da soggetti terzi.

**Il rischio di perdere il potere di controllo sui dati aziendali**

Inevitabile è, dunque, una perdita, quantomeno parziale, del potere di controllo su quei dati, con tutti i rischi che ciò comporta, in particolare ove la infrastruttura cloud venga utilizzata anche per la conservazione di informazioni aziendali strategiche o, comunque, di natura confidenziale. È bene, quindi, che chi sceglie il cloud – al fine di poter adottare per tempo le opportune cautele - sia consapevole, per un verso, dei rischi che si assume e, per altro verso, delle possibili responsabilità alle quali si espone nei confronti di terzi (clienti, fornitori, dipendenti, etc.) per eventuali violazioni della normativa in materia di privacy.

La domanda che ci si dovrebbe porre per il caso di violazione delle banche dati gestite attraverso una piattaforma cloud da un terzo fornitore è: come tutelare la società cliente nei confronti del fornitore? E quali sono le responsabilità nei confronti dei terzi i cui dati personali sono stati violati?

**Il tema va affrontato in una prospettiva internazionale**

Il tema credo debba essere affrontato in una prospettiva internazionale, in considerazione del fatto che il mercato del cloud è affollato da player globali e la nuvola può essere costituita da reti di data center localizzati in svariati Paesi europei ed extraeuropei. Il primo problema sarà, dunque, capire quale legge regoli i rapporti con il provider, sotto il profilo della tutela dei dati personali, e quale giudice potrebbe essere adito, qualora fossero state riscontrate delle inadempienze da parte del fornitore. In tale prospettiva, non credo sia neutra, specie in termini di costi legali, la circostanza di poter agire avanti ad un giudice nazionale o avanti ad una Corte della California. Per evitare sorprese per quanto concerne la giurisdizione competente, sarà, quindi, utile negoziare una previsione contrattuale sul punto.

Parimenti importante sarà l'individuazione della legge applicabile. È un dato notorio che il quadro normativo europeo in materia di protezione dei dati personali (fondato sulla Direttiva 95/46/CE) offre tutele giuridiche in materia di privacy che i Paesi extra UE - Stati Uniti compresi - in molti casi non sono in grado di assicurare.

**In Europa la normativa di dettaglio varia da paese a paese**

Peraltro, anche in ambito europeo - seppur in presenza di un nucleo centrale di principi condivisi - la normativa di dettaglio varia da Paese a Paese – in base al maggiore o minore rigore adottato da ciascuno Stato in sede di recepimento della direttiva comunitaria - così come variano i relativi adempimenti a cui è tenuto il titolare al fine garantire una piena compliance al trattamento di dati personali posto in essere. La Francia non consente, ad esempio, in assenza di una specifica autorizzazione, amministrativa, il trasferimento di dati sensibili (ad esempio, i dati relativi alla salute) al di fuori dei confini nazionali; differenti sono, poi, le regole adottate da ciascun Paese europeo in materia di data retention, con la previsione di diversi tempi massimi di conservazione dei dati.

In base alla Direttiva 95/46/CE ed al nostro Codice Privacy (Decreto Legislativo n.196 del 30 giugno 2003), l'individuazione della legge applicabile viene determinata in base a criteri essenzialmente territoriali che mal si conciliano con la nuvola: ovvero il principio dello stabilimento del titolare, o, comunque, l'utilizzo di strumenti presenti sul territorio europeo. Il semplice spostamento della sede della società e dei data center al di fuori del territorio europeo potrebbe, quindi, consentire al provider di sottrarsi ai vincoli previsti in materia di privacy dalla normativa comunitaria, anche laddove i propri servizi fossero diretti principalmente al mercato europeo. In tali circostanze, appare auspicabile una accorta selezione del provider, anche attraverso una chiara mappatura della rete di data center ove i dati della società potrebbero essere ospitati.

La normativa europea e quella italiana vietano, infatti, il trasferimento di dati personali verso Paesi extra Ue che non assicurano un adeguato livello di protezione, salvo che – prima di procedere al trasferimento - non vengano adottate adeguate salvaguardie, anche di natura contrattuale, per la protezione dei dati personali. Per il caso in cui l'infrastruttura del provider sia costituita da una rete di data center localizzati in diversi Paesi extra Ue – al fine di non esporsi a possibili rischi legali nei confronti dei propri clienti, dipendenti e fornitori – la società cliente, prima di inviare i dati personali di questi ultimi sulla nuvola, dovrebbe assicurarsi che il trasferimento dei dati aziendali da

Paese a Paese avvenga sempre nel rispetto di quelle garanzie minime di sicurezza previste dalla legge europea.

Peraltro, tra gli strumenti negoziali approvati dalla Unione Europea, l'adozione del set di clausole contrattuali standard per il trasferimento di dati da un titolare Ue ad un responsabile extra Ue, sembra essere il solo ad adattarsi alle specifiche esigenze del cloud.
Gli strumenti negoziali alternativi appaiono, infatti, difficilmente adattabili al cloud: le Binding Corporate Rules – ovvero le regole per i trasferimenti internazionali di dati infragruppo - non sono suscettibili di applicazione per i trasferimenti all'esterno di un medesimo gruppo societario ed i principi del Safe Harbor – il protocollo che regola i trasferimenti di dati verso gli Stati Uniti – non sono estensibili ad altri Pesi extra Ue. Peraltro, l'Autorità Garante tedesca – con una pronuncia del 18 giugno 2010 - si è espressa nel senso di ritenere i principi sanciti dal Safe Harbor non idonei ad offrire adeguate garanzie di protezione dei dati nel contesto dei servizi cloud. Anche sotto questo profilo, indispensabile appare una accurata mappatura della rete di data center ove i dati trasferiti potrebbero essere ospitati.

La trasparenza della piattaforma del fornitore è estremamente rilevante anche per una ulteriore ragione: la presenza fisica dei server in uno Stato comporterà per l'Autorità Giudiziaria di quello Stato la possibilità di dare esecuzione ad ordini di esibizione, di accesso o di sequestro, ove sussistano i presupposti giuridici in base alle leggi di quel Paese. Per converso, rispetto a quei medesimi database, l'Autorità Giudiziaria italiana potrà conseguire i medesimi risultati solo a mezzo di complicate rogatorie internazionali. Non è, quindi, indifferente per una società o per un ente pubblico sapere che i propri dati si trovino in un server in Italia, in Europa o in un imprecisato Paese extraeuropeo. Non a caso, il Presidente dell'Autorità Garante per la Privacy, **Francesco Pizzetti**, nella sua relazione annuale ha posto l'attenzione proprio sul tema del cloud computing, osservando che: «Occorre riflettere anche sui rischi che pone la nuova tecnologia del "cloud computing", con la quale i dati verranno sempre più sottratti alla disponibilità materiale di chi li produce e usa, e gestiti da enormi server collocati in ogni parte del pianeta. Un fenomeno che moltiplicherà i servizi di "remote hard disk" e renderà sempre più ampio il ricorso all'outsourcing e all'hosting dei sistemi, moltiplicando i servizi forniti da terzi secondo modalità che favoriscono sempre di più la delocalizzazione dei dati conservati. Si tratta di una nuova frontiera che allarma tanto le strutture militari quanto quelle di sicurezza interna, e che coinvolge problemi di enorme portata».

**Occhio all'operatore a cui si affidano i dati**
Al fine di contenere i possibili rischi, appare, dunque, imprescindibile un'accorta individuazione dell'operatore al quale i propri dati saranno affidati, anche attraverso una valutazione della solidità finanziaria e del grado di trasparenza e di sicurezza garantito dalle policy aziendali del partner prescelto. È consigliabile altresì l'adozione di adeguati strumenti negoziali che assicurino capienti garanzie nonché obblighi di notificazione per il caso di perdita o di accesso non autorizzato ai dati affidati in custodia. È importante, inoltre, che nel contratto siano contenuti precisi parametri che, attraverso la definizione di livelli di servizio minimi qualitativi e quantitativi (i cosiddetti "Service Level Agreements"), permettano di misurare le prestazioni del fornitore e le misure di sicurezza garantite. Così come saranno opportune – onde scongiurare rischi di lock in - clausole che disciplinino i tempi e le modalità di transizione dei data base da un fornitore ad un altro, nel caso di risoluzione o cessazione del contratto, con una precisa individuazione delle obbligazioni gravanti sul fornitore al termine del rapporto.
**Definizione dei poteri e delle responsabilità dei soggetti coinvolti**
Oltre ai profili qui considerati, il passaggio al cloud computing comporta una riflessione ulteriore con riguardo alla definizione dei poteri e delle responsabilità dei soggetti coinvolti.
La struttura stessa della nuvola sembra, infatti, scardinare le categorie tradizionali, disciplinate dal Codice Privacy, di titolare e responsabile del trattamento dei dati personali, ove il titolare è il soggetto a cui è riservato ogni potere decisionale con riguardo alle finalità ed alle modalità del trattamento dei dati; mentre il responsabile rappresenta il soggetto a cui il titolare delega alcune specifiche operazioni di trattamento, sulla base di istruzioni impartite dal titolare stesso.

**Il fornitore di servizi di cloud computing appare una figura ibrida**
Essendo questo il quadro normativo, il fornitore di servizi di cloud computing appare una figura ibrida: non è titolare del trattamento, ma mero custode delle banche dati delle società clienti. D'altro canto, la natura del servizio reso comporta un grado di autonomia incompatibile con il ruolo di esecutore delle istruzioni impartite dal titolare.
In una società in cui i dati saranno sempre più spesso custoditi da soggetti terzi, in prospettiva, appare auspicabile un intervento normativo volto a ridistribuire i pesi di responsabilità tra i diversi player, attraverso l'introduzione di una speciale figura di responsabile, che - a fronte di una sfera di autonomia particolarmente ampia, come quella occorrente per la gestione della nuvola - sia in grado di offrire ai clienti particolari garanzie in termini di affidabilità e di assumersi in prima persona specifiche responsabilità.
Mi pare, dunque, occorra interrogarsi sulla opportunità di individuare a livello europeo garanzie minime, che dovranno essere offerte dagli operatori che intendano offrire servizi di cloud, così come avviene in altri settori regolamentati - come possono essere il settore bancario ed il settore assicurativo - le cui attività comportano dei

rischi che non è lecito trascurare, non solo sotto il profilo della sicurezza - come peraltro già previsto dalla Direttiva 140/2009/CE nei confronti di tutte le imprese che forniscono servizi di comune elettronica accessibili al pubblico – ma altresì sotto il profilo della solidità finanziaria.

Per quanto l'imposizione di vincoli regolamentari possa essere percepita come un freno allo sviluppo del cloud, credo che – mai come in questo caso – la certificazione della affidabilità del provider possa rappresentare un passaggio necessario al fine di creare nel mercato quelle condizioni di fiducia che consentano di vincere le resistenze anche dei soggetti più cauti nell'affidarsi alla nuvola.

**Cloud computing e privacy**

La Commissione Europea, in una recente comunicazione al Parlamento "A comprehensive approach on personal data protection in the European Union", ha individuato il cloud computing - unitamente ai social network - tra i fenomeni emergenti che rendono non più differibile una radicale revisione del quadro normativo comunitario in materia di privacy, al fine di adeguare le regole e le categorie giuridiche esistenti a nuovi modelli di condivisione e di gestione dei dati personali, il cui sviluppo ha di fatto scardinato la capacità di tenuta dell'impianto normativo esistente.

Ad ogni modo, in attesa di interventi che adattino la normativa esistente in materia di privacy alle sfide che il mercato pone nel settore del cloud computing, credo che rilevanti fattori di competitività per i provider potranno essere:

(i) la trasparenza, sia al momento della instaurazione della relazione contrattuale (con riguardo alla mappa dei data center e alla policy privacy), sia in costanza di rapporto (attraverso la pronta notificazione di eventuali accessi abusivi);

(ii) l'offerta di adeguate garanzie in termini di misure di sicurezza (anche mediante certificazioni di enti accreditati);

(iii) l'offerta di adeguate garanzie patrimoniali per il caso di accesso abusivo, sottrazione o perdita di dati.

5 gennaio 2011