Privacy nel
questioni c

Fino ad un paio di anni fa si sentiva spesso dire che non fosse importante dove risiedessero i propri dati e che finalmente ci si poteva affrancare dall'infrastrutura e dalla sua gestione.

Semplicemente i dati erano nel "cloud" e gli utilizzatori non se ne dovevano preoccupare. In realtà la cosa non è così semplice per una serie di motivi. Il primo riguarda l'aderenza a leggi e regolamenti, come quando si trattano i dati personali dei propri dipendenti, clienti, fornitori ecc. Infatti la legge italiana sulla Privacy e numerosi provvedimenti del Garante in ambiti specifici prevedono una serie di limitazioni all'esportazione dei dati all'estero (in Europa, in Paesi equiparati, negli USA con il "Safe Harbor" e nel resto del mondo) e specifiche misure di sicurezza. Di questa difficoltà ha preso coscienza anche il legislatore europeo che, nella recente proposta di riforma della normativa di protezione dei dati personali, riesce contemporaneamente a semplificare le norme per chi deve sottostarvi (ad esempio le regola dello "stabilimento principale") e dall'altra ad aumentare i diritti e le garanzie dei cittadini europei (ad esempio il diritto all'oblio e l'applicazione del diritto UE ai cittadini UE fuori dal territorio comunitario).

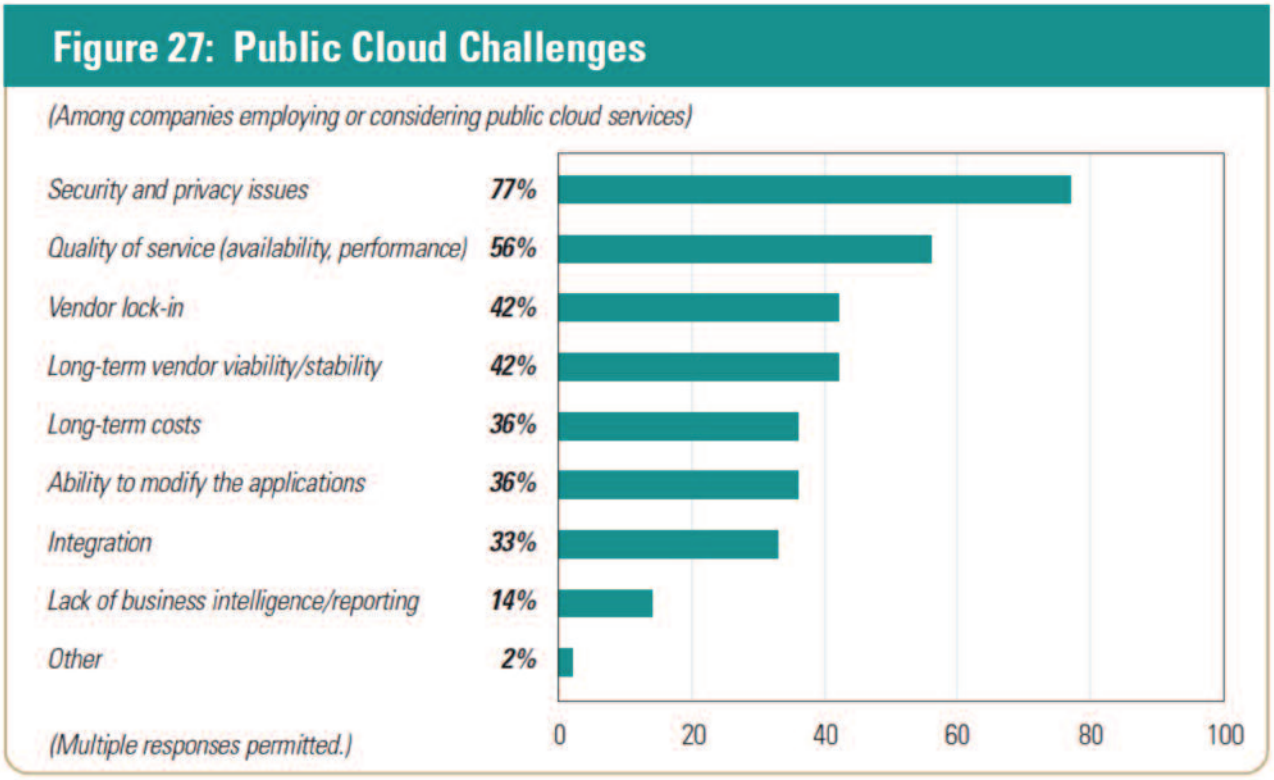
Il secondo motivo sta principalmente nel rischio di riservatezza non legato ai dati personali già protetti dalla Privacy. Ovvero alla possibilità che i propri dati, di qualunque natura essi siano, come ad esempio i propri segreti industriali, una volta depositati nel Cloud possano essere letti da persone non autorizzate. Potremmo qui parlare di spionaggio industriale, perdita accidentale di riservatezza in contesti dove ci si deve affidare a terzi per le misure di sicurezza, oppure di accesso da parte delle autorità di Paesi stranieri senza la protezione e l'autorizzazione di giudici italiani.

Che il cloud sia più insicuro del proprio data center, a volte gestito senza le adeguate risorse, soprattutto nel caso della PMI italiana, è in genere falso. In ogni caso una survey condotta

l Cloud: aperte

nel 2011 da un'organizzazione indipendente di aziende utenti Oracle (in figura) considera la Sicurezza e la Privacy essere la prima causa di preoccupazione dell'uso di servizi nel Public Cloud. Questo dà lo spunto per ulteriori considerazioni, la prima delle quali è che c'è Cloud e Cloud. Quanto detto è infatti sicuramente vero per il Public Cloud e non pertinente rispetto al Private Cloud, dove l'infrastruttura è gestita presso l'azienda stessa (Domestic Cloud) o un suo outsourcer a lei dedicato (assomigliando così molto all'outsourcing già ben conosciuto e raramente criticato sotto questo profilo). La seconda considerazione riguarda i destinatari dei servizi Cloud. Osserviamo che quando chi utilizza il cloud è un privato (B2C), la richiesta di riservatezza non viene assolutamente posta. Come individui, la maggior parte di noi non si cura di tali aspetti in cambio di servizi sempre migliori e a nessun costo apparente. C'è inoltre il caso del Community Cloud, che essendo utilizzabile da gruppi di aziende simili per certi interessi e necessità, potrebbe migliorare gli aspetti di sicurezza e controllo senza perdere completamente i vantaggi legati alle economie di scala, efficienza e qualità rese possibili da questi nuovi modelli. Ciò rappresenta una grande opportunità per la Pubblica Amministrazione italiana, in grado così di intraprendere il consolidamento dei Data Center utilizzando questo "deployment model" che garantirebbe risparmi ed efficienze senza dover rinunciare a compliance e controllo. Osserviamo che l'industria privata consolida da diversi anni il data center e le sue applicazioni (la single instance, il grid, la virtualizzazione ecc.); in ambito pubblico, il (Community) Cloud potrebbe garantire queste efficienze senza compromettere l'autonomia di indirizzo e di governo dei diversi attori della sanità e della pubblica amministrazione locale.

ALESSANDRO VALLEGA
Security Business Development Manager Oracle Italia
Consiglio Direttivo Clusit



Enterprises Advance into the Cloud: 2011 IOUG Survey on Cloud Computing *was produced by Unisphere Research and sponsored by Oracle.*

Nei mesi scorsi si è costituito, con 26 persone appartenenti a 15 tra aziende ed associazioni professionali, un Gruppo di Lavoro sul tema della Privacy nel Cloud. Tale gruppo di lavoro, organizzato nell'ambito di Oracle Community for Security[1], ha articolato una serie di raccomandazioni che si trovano raccolte in un libretto di una sessantina di pagine liberamente scaricabile da questo indirizzo: https://privacycloudmobile.clusit.it/. Per inciso si noti che allo stesso indirizzo si possono scaricare dei lavori analoghi sulla salvaguardia della Privacy in caso di utilizzo di dispositivi *mobile*, sulla sicurezza del Fascicolo Sanitario Elettronico e sul Ritorno dell'investimento in Sicurezza Informatica.
Nel lavoro svolto si è assunto il punto di vista di un'azienda italiana titolare dei trattamenti soggetti alla legge sulla Privacy, avendo cura di considerare il quadro normativo specificamente italiano. In questo senso il documento è un elemento di novità in quanto si discosta dalla bibliografia internazionale sia per la lingua sia per il contesto. Il tema è stato trattato in maniera ampia, grazie alle competenze multidisciplinari del gruppo di lavoro, sotto diversi aspetti, nella fattispecie legale, contrattuale, tecnologico, organizzativo e di audit.

RESPONSABILE VS TITOLARE: nel caso del Cloud le competenze del titolare (che a norma di legge riguardano le *decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*) appaiono sproporzionate rispetto al suo potere di decidere come fare le cose (nello specifico di decidere quali misure di sicurezza adottare e la necessità di effettuare delle verifiche e degli audit), soprattutto in presenza di grandi cloud provider stranieri contrapposti a piccoli titolari italiani della PMI. Tali soggetti infatti – normalmente - prevedono contratti standard non negoziabili nei contenuti ma eventualmente solo nel prezzo. Quindi la tentazione di alcuni è di considerare "titolare" il cloud provider e quindi scaricarsi di una serie di responsabilità.
Putroppo, allo stato attuale della norma, tale soluzione non è praticabile ed esplicitamente esclusa anche nel recentissimo Vademecum sul Cloud Computing pubblicato dall'Autorità Garante della Privacy[2]. Nella già menzionata proposta europea di modifica normativa, tale situazione potrebbe forse cambiare grazie alla figura del joint-controller.
All'interno di questo tema si colloca anche quello delle catene di subfornitura e lo specifico provvedimento degli amministratori di sistema, per il quale il titolare dovrebbe conoscere gli amministratori di sistema del provider e dei suoi subfornitori. Un miglioramento possibile, per un'Europa che dichiara il Cloud essere strategico, potrebbe essere

quello che un ente centrale, legalmente riconosciuto, si faccia carico di verificare che i servizi dei cloud provider siano compliant rispetto alla Privacy svincolando da tale onere la PMI.

CONTRATTO: per quanto detto in precedenza sulle misure di sicurezza e sull'audit, ma anche per altri motivi, si è ritenuto di evidenziare l'importanza del controllo e della negoziazione di alcuni aspetti contrattuali, pur con le difficoltà già accennate. Nella fattispecie, con il quadro normativo attuale la responsabilità delle misure di sicurezza rimane sempre in capo al titolare e quindi non possono essere trascurate. Inoltre non sono accettabili alcune formulazioni in merito alla proprietà dei dati, alle modifiche unilaterali delle condizioni d'uso del servizio, alle condizioni di recesso e di termine del contratto ecc.
Prima di affidare parte dei propri processi di business ad un provider, un'azienda deve assicurarsi che anche il provider abbia dei limiti rispetto alla terminazione del servizio, vengano garantiti dei tempi adeguati e forniti degli strumenti tecnologici per poter migrare i propri dati in caso di fallimento della relazione. Infine è necessario prevedere contrattualmente ed organizzativamente alcune procedure che normano la comunicazione tra il titolare e il cloud provider nel caso di incidenti di sicurezza. Bisogna sapere che in ultima analisi dovranno essere informati nel modo più opportuno i clienti del titolare, oppure essi potranno scoprirlo autonomamente a mezzo stampa anche in ragione della moltitudine di titolari gestiti dallo stesso fornitore, con un più severo impatto sull'immagine aziendale.

MISURE DI SICUREZZA: la legge descrive dettagliatamente alcune misure di sicurezza "minime", la cui non osservanza comporta conseguenze di maggior impatto per il titolare che non le attui, e altre "idonee", la cui adozione dipende da un'analisi dei rischi anche in relazione "alle conoscenze acquisite in base al progresso tecnico". Le prime dovrebbero essere modificate nel tempo per via legislativa, cosa peraltro non ancora successa, e le seconde valutate caso per caso da chi le deve attuare ed eventualmente messe in discussione nel processo civile, in caso di contenzioso, tramite il giudizio di esperti e periti e il confronto con le best practice. In entrambi i casi le misure possono essere tecnicamente adottate solo tramite una stretta collaborazione tra cliente e fornitore e in base a dei confini che cambiano a seconda del modello di servizio (IaaS, PaaS e SaaS) e dell'ambito applicativo. Non è possibile dare per scontato che sia il fornitore a farsene carico. Nel documento[3] della Community si trovano alcune considerazioni secondo questa traccia. Inoltre vengono suggerite delle misure di validità abbastanza generale da poter essere considerate una nuova proposta di misure minime in ambito cloud. Esse sono:

1. Utilizzare solo reti e protocolli sicuri per la trasmissione dati tra la propria azienda e il provider.
2. Criptare il dato a riposo nel database e criptare lo storage e la trasmissione dati tra lo storage e il dbms.
3. Richiedere al provider di dare evidenza e di procedere alla criptazione del file system.
4. Rimuovere la chiave di criptazione dalla disponibilità del cloud provider.
5. Richiedere al provider forme di autenticazione federata per poter autenticare autonomamente i propri utenti.
6. Automatizzare le operazioni relative alla rimozione di utenti non più autorizzati tramite tecnologie di identity provisioning. (...)
7. Richiedere il tracciamento delle attività degli amministratori di sistema (...).
8. Normare le procedure per la notifica di qualsiasi evento di sicurezza.

Il Profilo di Alessandro Vallega si trova qui: https://www.securitysummit.it/relatori/view/224 ■

1 http://www.oracle.com/it/technologies/security/partner-171975-ita.html
2 http://www.garanteprivacy.it/garante/document?ID=1895296
3 https://privacycloudmobile.clusit.it/pages/Download.html