Lo stato dell'arte della disciplina legale del cloud, dal Garante della Privacy italiano al Working party 29, con uno sguardo veloce al futuro che ci aspetta.

di Bianca Del Genio

LA PROTEZIONE DEI DATI PERSONALI NEL CLOUD

Bianca DEL GENIO *è Direttore Affari legali e istituzionali di Microsoft Italia. In questo ruolo, si occupa in particolare di affari societari e compliance, affari regolamentari, contrattualistica commerciale. Partecipa come speaker a conferenze sugli aspetti legali e di compliance del cloud, Internet of things, Big Data, tematiche relative a ICT. Prima di Microsoft, ha ricoperto per 14 anni il ruolo di General Counsel di un gruppo multinazionale attivo nel settore dei servizi per la telefonia mobile.*

Secondo lo studio dell'istituto Forrester Research, la spesa per i servizi cloud nel 2016 potrebbe raggiungere i 106 miliardi di dollari nel mondo, il che significa un aumento del 21% rispetto ai livelli di spesa registrati nel 2015. Lo studio del Computer World Forecast 2015 ha trovato che, ad oggi, le iniziative di cloud computing sono i progetti più importanti per la maggioranza dei dipartimenti IT. Il passaggio al cloud sta avvenendo per svariate buone ragioni: il modello di costo basato sull'uso effettivo del servizio, l'accesso globale da qualsiasi luogo o *device*, la possibilità di aumentare o diminuire l'uso del servizio a seconda dell'andamento del proprio business, il fatto che abbia in sè la funzionalità del *disaster recovery* e che fornisce all'IT grande flessibilità nel rispondere alle necessità di sviluppo e di business. Dal momento che tutte queste promesse sono rispettate, le società stanno lavorando per aumentare il ricorso al cloud e renderlo parte integrante della strategia di gestione del proprio business.

Allo stesso modo, però, c'è molto timore ad approcciare il cloud in quanto aleggiano importanti questioni circa la protezione dei dati personali, la sicurezza degli stessi e la compliance su cui c'è bisongo di maggiore trasparenza.

In relazione alla problematica della protezione dei dati personali, è evidente che il cloud pubblico pone dei quesiti particolari: il cloud è un ambiente di dimensioni enormi, in cui sono ospitati i dati appartenenti a soggetti plurimi; è un luogo remoto, anche geograficamente, che dà già per questo, l'idea di perdita di controllo dei dati in esso conservati, degli accessi ai dati stessi e dell'uso che di quei dati si può fare. Molti dubbi legati alla privacy poi, si riferiscono ai comportamenti dei governi. Da quando nel 2013 è stato rivelato il programma di sorveglianza massiva da parte del governo americano, l'interesse al tema della privacy si è acutizzato e ovviamente il cloud è stato messo sotto strettissimo esame. I fornitori di servizi cloud hanno iniziato a rendere pubblici i loro problemi nella gestione delle richieste dei governi ad avere accesso ai dati personali dei clienti e stanno chiedendo a gran voce delle riforme serie delle pratiche di sorveglianza dei governi. D'altro canto, le aziende sono di certo entusiaste nell'adottare le soluzioni innovative che il cloud permette loro, ma sono altresì preoccupate di non perdere il controllo dei loro dati personali, di conservarne la proprietà e di essere responsabili di qualcosa che non possono controllare. Molte aziende quindi vogliono sapere il luogo in cui i propri dati personali risiederanno e come saranno controllati gli accessi ai loro dati quando questi saranno nel cloud. La sensibilità al tema è talmente alta che da una recente indagine condotta da Microsoft risulta che il 75% delle aziende ha confermato che l'obbligo primario che sentono in questo momento è quello di proteggere la privacy dei loro clienti oltre gli interessi nazionali.

Infine, non possiamo non menzionare fra le premesse importanti di questo approfondimento, il problema chiave che è quello relativo al trasferimento dei dati personali al di fuori dell'UE: negli ultimi mesi abbiamo assistito alla rivoluzione causata dalla sentenza della Corte di Giustizia Europea che ha dichiarato invalido l'accordo di Safe Harbor che negli ultimi 15 anni ha regolamentato e permesso i trasferimenti dei dati personali dall'Europa verso gli Stati Uniti e intorno al quale si sono sviluppati interi business se non aziende stesse, tra le più grandi e capitalizzate al mondo. Il problema generato dalla sentenza della Corte di Giustizia è solo parzialmente risolto alla data di pubblicazione di questo articolo, ma ne parleremo più avanti.

Cosa gli utenti si aspettano da un cloud provider

Per anni abbiamo assistito ad un racconto delle funzionalità del cloud in cui sembrava che la caratteristica principale di questa tecnologia fosse, oltre all'economicità, il fatto che non ponesse alcun problema giuridico circa la protezione dei dati personali. Sembrava infatti, che il cloud fosse una sorta di "terra di nessuno", in quanto si presumeva che chi decideva di trasferire i dati nel

cloud, era consapevole e accettava il fatto che avrebbe perso ogni forma di controllo sui dati stessi e chi invece forniva il servizio di cloud, doveva solo assicurarsi che il concetto di cloud fosse quanto più vago e lontano possibile per i propri clienti. Gli esperti di diritto per anni hanno posto domande, organizzato convegni, cercato di approfondire il tema soprattutto dal punto di vista tecnico, ma la risposta classica era che il significato di cloud, non solo letterale, era proprio nuvola e quindi luogo-non-luogo in cui non si poteva nemmeno immaginare di poter applicare delle leggi.

In realtà questo atteggiamente ha fatto crescere presso i consumatori una forte diffidenza nei confronti della tecnologia in cloud, che si è manifestata in un grande ritardo nell'adozione della stessa che in alcuni Paesi del mondo è più marcato che in altri. In una indagine commissionata da Microsoft nel 2013, i consumatori avevano espresso chiaramente la loro preoccupazione in merito alla tutela della privacy e della sicurezza da parte dei *cloud providers* e in merito al rischio percepito di perdere il controllo dei propri dati se questi fossero stati trasferiti sul cloud. Nella stessa indagine, però, risultava che i consumatori che avevano già adottato il cloud erano, in stragrande maggioranza, molto soddisfatti perchè ritenevano che le misure di sicurezza, applicate ai loro dati personali presenti sul cloud, erano di certo molto superiori rispetto a quelle che loro stessi erano in grado di adottare per proteggere gli stessi dati sulle tecnologie tradizionali. Era quindi evidente che occorreva iniziare a raccontare una storia diversa sul cloud, la storia vera, quella che dimostra che la tecnologia in cloud è una tecnologia molto sicura e che si può gestire nel pieno rispetto delle normative applicabili, incluse quelle cui i singoli clienti sono tenuti per obblighi di compliance.

Cosa i regolatori e i legislatori hanno fatto in Europa e in Italia

Già dal 2011, le Istituzioni Europee e quelle italiane iniziano a studiare il fenomeno del cloud. Con il manuale per l'utilizzo consapevole dei servizi di cloud computing, il Garante privacy italiano nel 2011 apre la strada all'analisi della piattaforma di cloud e chiama tutte le autorità internazionali a lavorare per disciplinare questo servizio di cui il Garante italiano intravede le grandi potenzialità e il grande impatto di business. In quel documento, il Garante invita coloro che stanno guardando al *cloud computing* come soluzione IT per il proprio business, tra le altre cose, a valutare prioritariamente rischi e benefici della soluzione offerta, verificare l'affidabilità del fornitore, privilegiare i servizi che ammettano la portabilità dei dati, assicurarsi di conservare la disponibilità dei propri dati in caso di necessità, non perdere di vista i dati ed informarsi sul luogo in cui i dati risiedono e non ultimo valutare attentamente le condizioni contrattuali.

Il 7 luglio 2012, il Working Party 29, il gruppo di lavoro dei Garanti Privacy che si riunisce a Bruxelles, adotta un parere sul cloud computing in cui ribadisce chiaramente che "*imprese e amministrazioni che intendono utilizzare servizi di cloud computing dovrebbero innanzitutto effettuare un'analisi del rischio completa e approfondita. Tutti i fornitori di servizi cloud nel SEE dovrebbero fornire al cliente tutte le informazioni necessarie per valutare correttamente ipro e i contro dell'adozione di un simile servizio. Sicurezza, trasparenza e certezza-giuridica per i clienti dovrebbero essere principi fondamentali alla base dell'offerta di servizi di cloud computing*".

Con la Mini Guida pubblicata dal Garante italiano nel 2012 e intitolata "Cloud Computing: proteggere i dati per non cadere dalle nuvole", il Garante mette a disposizione un decalogo verso coloro che sono interessati alle soluzioni in cloud: dieci regole che il Garante consiglia di rispettare e far rispettare per evitare che le soluzioni in cloud si trasformino in tecnologie in cui il diritto fondamentale delle persone, come quello alla privacy, sia dimenticato se non addirittura violato. Fra le dieci regole elencate nella mini guida, il Garante ribadisce i suggerimenti già espressi nel manuale del 2011 sottolineando l'importanza del cosiddetto risk assessment che gli utenti del cloud sono invitati a fare prima di migrare i dati personali presso un cloud provider e che anzi dovrebbe costituire la *condition sine qua non* affinchè gli utenti scelgano un cloud provider invece che un altro. Pretendere dal cloud provider il rispetto di certe misure di sicurezza, l'uso di personali altamente formato, il persistere del controllo dei dati da parte del cliente, seppur a condizioni che non mettano in pericolo la sicurezza della piattaforma, sono solo alcuni dei suggerimenti che il Garante elenca e spiega nel dettaglio, confermando la consapevolezza dell'importanza e delll'irrevocabilità del passaggio al cloud computing.

Il 26 ottobre 2012 durante la 34° conferenza internazionale delle Autorità per la protezione dei dati personali, viene pubblicata una decisione in cui le Autorità dichiarano che è vero che il *cloud computing* sta diventando sempre più attrattivo a causa della promessa di efficienza economica, di basso impatto ambientale, di semplificazione e di facilità d'uso, ma è anche vero che il *cloud computing* sta sollevando una serie di importanti questioni in relazione, per esempio, al fatto che si tratta di una tecnologia ancora in evoluzione, che il trattamento dei dati personali è diventato un processo globale, che manca la trasparebza nelle modalità di gestione dei dati personali e questo rende ovviamente difficile se non impossibile proteggere i cittadini e il loro diritto alla protezione dei dati personali. Pur plaudendo alle diverse iniziative di verifica che diverse autorità e istituzioni internazionali avevano già iniziato a condurre sul tema, la 34° conferenza internazionale delle Autorità si espone a fornire delle linee guida che possiamo riassumere come segue: il cloud computing no può significare una riduzione o un annullamento dei principi posti a protezione dei dati personali e i cloud provider sono, perciò, tenuti a garantire in maniera appropriata e con la massima trasparenza l'adozione di tutte le misure necessarie, per non violare il diritto alla sicurezza e alla protezione dei dati personali dei loro clienti.

Nello stesso tempo, le istituzioni europee e italiane si esprimevano affinchè tutte le aziende lavorassero per rendere i propri servizi in linea con le normative applicabili in tema di protezione dei dati personali. Nel 2014, Viviane Reding, l'allora vice president della Commissione Europea per la Giustizia, i diritti fondamentali e la cittadinanza, aveva infatti detto "*some companies and a few governments continue to see data protection as an obstacle rather than as a solution; privacy rights as compliance costs, and not as an asset*" (trad. alcune società e alcuni governi continuano a vedere la protezione dei dati personali come un ostacolo più che una soluzione; i diritti alla privacy come un costo di compliance più che come un asset).

Cosa la tecnologia in cloud è in grado di offrire ai clienti in termini di protezione dei dati personali

L'offerta in cloud è ai nostri giorni di certo un'offerta evoluta, anche sotto il profilo giuridico. Tutti i cloud provider più grandi e solidi hanno investito negli ultimi anni per mettere al sicuro il proprio prodotto in qualsiasi contesto giuridico nel mondo di fronte agli utenti e soprattutto di fronte ai legislatori e ai governi locali. Nei confronti dei consumatori, si è lavorato per rendere sempre più diretto e materiale il controllo da parte degli interessati sui propri dati.

Esistono sul mercato soluzioni in cloud che permettono ai clienti di sapere, e addirittura di scegliere preventivamente, il luogo in cui i dati risiedono, di sapere in ogni momento chi e perchè sta accedendo alla piattaforma e quindi ai loro dati personali; ci sono soluzioni cloud che garantiscono ai clienti che solo un certo tipo di personale, con certi livelli di autorizzazione, può di fatto avere accesso alla piattaforma e quindi ai dati e che comunque tutti gli accessi sono registrati e visibili da parte degli interessati.

Esistono soluzioni in cloud che garantiscono un sistema di criptazione molto esteso, che riguarda i dati quando sono fermi nei *data centers*, o quando si muovono da un sistema all'altro, o da un utente all'altro. Esistono offerte contrattuali molto serie, in cui il cloud provider fornisce garanzie più che solide nei confronti dei propri clienti: basti pensare alla possibilità che alcuni cloud provider americani offrono, di far sottoscrivere ai propri clienti, che risiedono in Europa, le Standard Model Clauses, clausole contrattuali che garantiscono al cliente l'adozione da parte del provider di adeguati livelli di protezione dei dati personali anche durante il trasferimento degli stessi al di fuori dell'Unione Europea, verso gli Stati Uniti, e che sottopongono alla legge del luogo in cui risiede il cliente tutti gli accordi contrattuali relativi al trattamento dei dati personali.

Esistono offerte in cloud che hanno ottenuto il riconoscimento ISO 27018, che assicura il cliente un controllo ulteriore sulle garanzie contrattuali fornite dal provider in quanto quest'ultimo è sottoposto ad audit annuali da parte di una società esterna ed indipendente, in merito ad alcuni obblighi che il provider assume e ciò senza alcun costo aggiuntivo per il cliente.

Esistono aziende che hanno sviluppato dei processi interni molto precisi e trasparenti per i clienti, che garantiscono che ai dati di questi ultimi non saranno autorizzati ad accedere terzi che non abbiano requisiti minimi di competenza e legittimità, e fra questi terzi sono inclusi i Governi. Il caso emblematico di questo tipo di approccio trasparente nei confronti dei clienti rispetto alle richieste di accesso di terzi è quello di Micosoft che ha portato in giudizio il governo americano per aver quest'ultimo chiesto l'accesso a dati personali di un utente dell'azienda senza rispettare la procedura prevista per richiedere tale attività. Il caso risale al 2013 e riguarda la richiesta di accesso da parte del governo americano ai dati di un utente di Microsoft, dati che risiedono nei data centers che l'azienda ha in Irlanda. Il governo anericano pretende di ottenere questi dati direttamente da Microsoft per il solo fatto di aver notificato a quest'ultima un ordine di accesso (cd. warrant) ed indipendentemente dal luogo in cui tali dati risiedono. Microsoft a sua volta rigetta la richiesta del governo americano in quanto irrituale e chiede che quest'ultimo applichi la procedura internazionale prevista per questo tipo di casi e chieda l'accesso al data center irlandese tramite autorizzazione dell'autorità competente sul territorio irlandese.

Il caso in questione è attualmente acora pendente dinanzi alla corte di secondo grado e nell'attesa della sua conclusione, Microsoft ha implementato delle procedure interne che garantiscono ai propri clienti che gli accessi ai loro dati saranno consentiti da parte di Microsoft al Governo americano solo nei seguenti casi e alle seguenti condizioni:

(i) Qualora Microsoft accerti la validità della richiesta di accesso; in particolare sarà valutato se il governo richiedente l'accesso è competente e se l'ordine è stato validamente indirizzato a Microsoft,

(ii) dopo che sia tentato, anche in via giudiziale, di chiedere al governo americano di rivolgersi direttamente al cliente.

(iii) Microsoft avrà fatto il possibile per ottenere che la richiesta di accesso sia comunicata anche all'utente, o nel caso di azienda, almeno a qualche funzione dell'azienda tenuta per dovere professionale alla confidenzialità (la funzione legal o quella di compliance, per esempio).

Scenari giuridici futuri

L'importanza del cloud nelle strategie di crescita delle aziende, sia nel settore pubblico che nel settore privato, è un elemento che ad un legislatore attento non può sfuggire. La dimensione del problema giuridico che il cloud pone, che è ovviamente una dimensione internazionale se non addirittura globale, è qualcosa di atrettanto evidente. Pensare ad un efficace presidio giuridico in materia di protezione dei dati personali nel cloud, quindi, deve necessariamente tenere conto della necessità che il legislatore o il regolatore lavorino attorno al tavolo con legislatori e regolatori degli altri Paesi, che si condividano i principi fondamentali e si dettino regole efficaci che rendano possibili e trasparenti alcuni tipi di trattamento che sono di fatto inevitabili, primo fra tutti il trasferimento dei dati da un Paese all'altro.

A tal proposito, plaudo, pur senza entrare nel merito per questioni di tempismo, il nuovo accordo che la Commissione Europea ha trovato con il Governo americano in sostituzione dello storico accordo Safe Harbor che per più di dieci anni ha garantito i trasferimenti transfrontalieri di dati e che qualche mese fa la Corte di Giustizia Europea aveva dichiarato invalido. Non si può pensare di impedire che l'innovazione tecnologica continui a progredire, ma si deve senz'altro trovare modi innovativi ed efficaci per regolamentare questo settore. Come anche **Brad Smith**, Presidente e General Counel di Microsoft usa ripetere, un nuovo Safe Harbor, la criptazione e la modernizzazione delle leggi in materia IT sono tra le sfide più importanti del mondo digitale e che, anche se in ritardo, il mondo non può fallire nel risolvere questi problemi così importanti. ©