12 dicembre 2012 13:07

Cloud computing. Rischi e vantaggi

di Deborah Bianchi

Il termine Cloud Computing indica *"infrastrutture IT che implicano l'archiviazione e l'elaborazione in remoto di dati e programmi in data center di fornitori (provider) cloud o in data center interconnessi, nonché l'accesso a servizi attraverso la rete web. Secondo l'Istituto Nazionale US sugli standard tecnologici (NIST), il cloud computing abilita dovunque, convenientemente e immediatamente, all'accesso tramite la rete a un bacino di archivi condivisi consistenti in risorse informatiche, come reti, server, archivi, applicazioni e servizi, che possono essere - con minimo impegno di gestione ed abilità informatiche - rapidamente messi in relazione ed interconnessi ai service provider*" (CCBE GUIDELINES ON THE USE OF CLOUD COMPUTING SERVICES BY LAWYERS ovvero LINEE GUIDA DEL CCBE SULL'UTILIZZO DEI SERVIZI DI CLOUD COMPUTING DA PARTE DEGLI AVVOCATI - September 2012, pag. 2-3).

Si tratta del concetto di internet-bene comune, risorsa primaria della società paragonabile all'avvento dell'energia elettrica o del petrolio. Il cloud riassume e sintetizza tutte le utilità offerte dalla Rete: la possibilità di fruire di contenuti a prescindere dal luogo in cui uno si trova; la possibilità di condividere documenti con tutti; la possibilità di diramare i propri comunicati stampa e i propri pensieri e commenti sui social network con un unico tocco di click.

Altro vantaggio lo registriamo nell'aspetto economico. Il cloud offre la possibilità all'utenza di avere accesso a capacità di storage (immagazzinamento dati) e di calcolo ad una frazione del costo che si dovrebbe affrontare per ottenere gli stessi risultati tenendosi tutta l'infrastruttura hardware e software in ufficio. Questo carattere si presta ad attirare l'attenzione delle imprese medio-piccole e degli Studi professionali.

I vantaggi offerti dai servizi captabili in Rete sono enormi. Pensiamo a servizi come:
- Scribd (http://www.scribd.com)(un servizio che offre la possibilità di archiviare, leggere e condividere documenti in rete. Documenti che possono essere postati via e.mail, social network e integrabili con il proprio sito web);
- Slideshare (http://www.slideshare.net)(un servizio che offre la possibilità di archiviare, leggere e condividere presentazioni create in PowerPoint, OpenOffice, Keynote. Condivisibili via LinkedIn, Facebook e Twitter. Slideshare è accessibile attraverso dispositivi e piattaforme mobile differenti: iPad, iPhone, Android. Attenzione a Slidecast: Slideshare (slides) + Podcast (mp3) che permette di aggiungere alle proprie presentazioni un file mp3 audio e sincronizzarlo con le slide. Con Slideshare è possibile inoltre inserire nelle presentazioni video pubblicati su YouTube);
- MailChimp (http://www.mailchimp.com)(un servizio di e-mail marketing che offre la possibilità di creare newsletter e gestire campagne di e-mail marketing ondine);
- qik (http:// www.qik.com)(un servizio di video streaming progettato e sviluppato per dispositivi mobili. Qik è un'applicazione che permette di registrare e condividere video in rete via social network, YouTube, e-mail e integrarli direttamente sul proprio sito o blog);
- Audioboo (http:// www.audioboo.fm)(un servizio di podcasting che offre la possibilità di registrare, archiviare e condividere in rete messaggi audio, documenti sonori);
- CardMunch (http://www.cardmunch.com)(un'applicazione per iPhone che permette la scansione e l'archiviazione di biglietti da visita. Tutti i contatti archiviati sono accessibili su CardMunch e sincronizzabili con la propria rubrica su iPhone).

Come sempre la tecnologia è delizia ma è anche croce. A fronte di questi innumerevoli vantaggi ci sono anche dei rischi. Che attengono essenzialmente a quattro aspetti:
1 - la responsabilità per la conservazione dei dati personali e delle informazioni aziendali o professionali riservate, che, come noto, nel cloud vengono trasferiti dall'utente su server remoti che non sono governati dalla volontà del

cliente;
2 - la qualificazione del contratto di servizi cloud quale snodo cruciale della distribuzione delle responsabilità e dei rischi che ne discendono per le parti;
3 - la tutela dei diritti dei terzi. Chi sarà responsabile per il sinistro privacy in danno del terzo? Il provider di servizi cloud o il cliente di quest'ultimo che ha fruito del servizio?
4 - la portabilità del patrimonio informativo aziendale o professionale da un fornitore di cloud ad un altro. Il cliente del servizio di cloud dev'essere libero di poter traslocare i propri dati da un fornitore a un altro senza rimanere vincolato da contratti elusivi di questa possibilità che una volta accalappiato l'utente non gli danno più la possibilità di andare da un competitor.
La prima preoccupazione di uno Studio legale che decide di servirsi del cloud dev'essere quella della tipologia di contratto (ossia SaaS, PaaS e IaaS) che va a stipulare. Si dovrà stare bene attenti alle condizioni offerte dal fornitore. Solo un'adeguata regolamentazione contrattuale infatti costituisce strumento di garanzia per un'equa ripartizione dei rischi e delle responsabilità tra il cliente e il provider cloud.

Il Garante per la protezione dei dati personali, per facilitare l'attività di aggiornamento e innovazione di imprenditori e P.A., ha realizzato un vademecum sul tema: "CLOUD COMPUTING - *Proteggere i dati per non cadere dalle nuvole", rivolto non solo agli esperti del settore, ma a tutti coloro che sono interessati alla comprensione e alla potenziale adozione di queste nuove tecnologie.*

"CLOUD COMPUTING - PROTEGGERE I DATI PER NON CADERE DALLE NUVOLE"La guida del Garante della Privacy per imprese e pubblica amministrazione.
NORMATIVA PRIVACY NELLE NUVOLE – SPUNTI DI RIFLESSIONE
In attesa di una normativa nazionale e internazionale aggiornata e uniforme, che permetta di governare il fenomeno senza rischiare di penalizzare l'innovazione e le potenzialità di sviluppo delle "nuvole" informatiche, è necessario che le imprese e la pubblica amministrazione, incluse tra l'altro le cosiddette "centrali di committenza" (soggetti che effettuano acquisti per una pluralità di pubbliche amministrazioni), prestino particolare attenzione ai rischi connessi all'adozione dei servizi di cloud computing, anche in relazione agli aspetti di protezione dei dati personali. **Il titolare e il responsabile del trattamento.** La pubblica amministrazione o l'azienda, "titolare del trattamento" dei dati personali, che trasferisce del tutto o in parte il trattamento sulle "nuvole", deve procedere a designare il fornitore dei servizi cloud "responsabile del trattamento" Questo significa che il cliente dovrà sempre prestare molta attenzione a come saranno utilizzati e conservati i dati personali caricati sulla "nuvola": in caso di violazioni commesse dal fornitore, anche il titolare sarà chiamato a rispondere dell'eventuale illecito. Il cliente di ridotte dimensioni, come una piccola impresa o un ente locale, **(o l'avvocato, nel nostro caso)** potrebbe tuttavia incontrare difficoltà nel contrattare adeguate condizioni per la gestione dei dati spostati "sulla nuvola". Anche in questo caso, non sarà però sufficiente, per giustificare una eventuale violazione, affermare di non avere avuto possibilità di negoziare clausole contrattuali o modalità di controllo più stringenti. Il cliente di servizi cloud, infatti, può sempre rivolgersi ad altri fornitori che offrono maggiori garanzie, in particolare per il rispetto della normativa sulla protezione dei dati. Il Codice della privacy prevede, tra l'altro, che il titolare eserciti un potere di controllo nei confronti del responsabile del trattamento (in questo caso il cloud provider), verificando la corretta esecuzione delle istruzioni impartite in relazione ai dati personali trattati. **Trasferimento dei dati fuori dell'Unione Europea.** Il Codice della privacy definisce regole precise per il trasferimento dei dati personali fuori dall'Unione europea e vieta, in linea di principio, il trasferimento "anche temporaneo" di dati personali verso uno Stato extraeuropeo, qualora l'ordinamento del Paese di destinazione o di transito dei dati non assicuri un adeguato livello di tutela. Questa evenienza può verificarsi frequentemente nel caso in cui si decida di usufruire di servizi di public cloud invece che di modalità private o ibride. Per le sue valutazioni il titolare del trattamento (in genere chi acquista servizi cloud) dovrà quindi tenere in debito conto anche il luogo dove vengono conservati i dati e quali sono i trattamenti previsti all'estero. Il trasferimento di dati verso gli Stati Uniti, ad esempio, può essere facilitato nel caso in cui il cloud provider aderisca a programmi di protezione dati come il cosiddetto Safe Harbor (letteralmente "porto sicuro"), un accordo bilaterale Ue-Usa che definisce regole sicure e condivise per il trasferimento dei dati personali effettuato verso aziende presenti sul territorio americano.Le limitazioni per il trasferimento dati all'estero incidono anche sugli spostamenti "infragruppo" di una multinazionale. In questo caso, la presenza di forti "norme vincolanti d'impresa" (binding corporate rules) a tutela dei dati personali può consentire l'eventuale trasferimento dei dati nel rispetto della privacy degli interessati. **Sicurezza dei dati.** Il titolare del trattamento deve assicurarsi che siano adottate misure tecniche e organizzative volte a ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, di

modifica dei dati in conseguenza di interventi non autorizzati o non conformi alle regole. Il cliente dovrebbe, ad esempio, accertarsi che i dati siano sempre “disponibili” (che si possa cioè sempre accedere ai dati) e “riservati” (che l’accesso cioè sia consentito solo a chi ne ha diritto).Per garantire che i dati siano al sicuro, non sono importanti solo le modalità con cui sono conservati, ma anche quelle con cui sono trasmessi (ad esempio utilizzando tecniche di cifratura). **I diritti dell’interessato**. I soggetti pubblici e le imprese che decidono di avvalersi di servizi cloud per gestire i dati personali dei loro utenti o clienti non devono dimenticare che il Codice della privacy attribuisce agli interessati (le persone a cui si riferiscono i dati) precisi diritti. Ad esempio, l’interessato ha diritto di conoscere quali siano i dati che lo riguardano in possesso dell’amministrazione pubblica o dell’impresa, per quale motivo siano stati raccolti e come siano elaborati. Può richiedere una copia intelligibile dei dati personali che lo riguardano, il loro aggiornamento, la rettifica o l’integrazione. In caso di violazione di legge, può esigere anche il blocco, la cancellazione o la trasformazione in forma anonima di queste informazioni. Il cliente del servizio cloud, in qualità di titolare del trattamento dati, per soddisfare queste richieste, deve poter mantenere un adeguato controllo non solo sulle attività del fornitore, ma anche su quelle degli eventuali sub fornitori dei quali il cloud provider potrebbe avvalersi”.