GIANNI·ORIGONI
GRIPPO·CAPPELLI
PARTNERS

# Sicurezza dei dati e dell'informazione all'epoca del *cloud*: gli aspetti pratici

**Avv. Daniele Vecchi**

**Studio Gianni, Origoni, Grippo, Cappelli & Partners**

# Il Cloud Computing

**«Cloud computing: modello per abilitare, tramite la rete, l'accesso diffuso, agevole e a richiesta, ad un insieme condiviso e configurabile di risorse di elaborazione (reti, server, memoria, applicazioni e servizi) che possono essere acquisite e rilasciate rapidamente e con minimo sforzo di gestione o di interazione con il fornitore di servizi.» (*National Institute of Standards and Technology* - NIST)**

Diversi modelli di servizio

- SAAS - *Software as a Service* (rende disponibili applicazioni informatiche, es. email, CRM, e-learning, archiviazione/back-up remoto);
- IAAS - *Infrastructure as a Service* (vere e proprie infrastrutture, es. server virtuali remoti);
- PAAS - *Platform as a service* (piattaforme informatiche, es. Google Apps Engine, Microsoft Windows Azure)

- *Private cloud*: infrastruttura informatica dedicata alle esigenze di una singola organizzazione, ubicata nei suoi locali o affidata in gestione ad un terzo (hosting dei server).
- *Public cloud*: infrastruttura di proprietà di un fornitore che mette a disposizione i propri sistemi attraverso l'erogazione via web di applicazioni informatiche, di capacità elaborativa e di stoccaggio.
- Hybrid cloud: modello in cui l'utente utilizza risorse sia del suo cloud privato che di un cloud pubblico.

  - Possibile **migrazione dei dati dai sistemi locali** sotto il diretto controllo dell'utente (es. impresa o studio professionale) ai **sistemi remoti del cloud provider**
  - Applicazioni per l'elaborazione dei testi, per la gestione di agende e calendari (anche condivisi), gestione delle relazioni coi clienti, cartelle per l'archiviazione dei documenti on-line, soluzioni esternalizzate di posta elettronica.
  - Esempi di cloud: *Salesforce.com*, IBM, Dropbox per storage online, Aruba (cloud italiano), Yahoo, Gmail per posta elettronica in cloud

# Vantaggi e svantaggi pratici

- Prospettive di maggiore efficienza economica, basso impatto ambientale, semplicità nelle operazioni di inserimento/storage, caratteristiche *user- friendly*
- Disponibilità di una potenza di elaborazione quasi illimitata, possibilità di accedere ai dati ovunque sia disponibile una connessione Internet
- Ottimizzazione dell'uso dell'hardware disponibile da parte dei providers tramite lo spostamento dei dati degli utenti (es. da un data center all'altro)
- Gli utenti non devono curarsi della gestione dei sistemi informatici, completamente gestiti dai cloud providers
- Soluzioni più flessibili, efficienti, adattabili ed economiche di quelle *in-house*

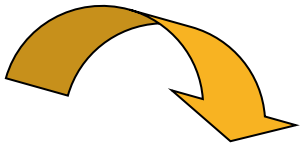
- Soggetti coinvolti nelle operazioni di gestione dei dati dell'utente spesso in tutto o in parte sconosciuti, rischi di "trattamenti a catena"
- Carenza di trasparenza sulle procedure di sicurezza adottate dal provider e difficoltà a condurre adeguati *risk assessment*
- Perdita di controllo dei dati e difficoltà di monitorare le attività del provider e i relativi profili di responsabilità
- Violazioni della riservatezza, integrità e disponibilità dei dati, nonché delle norme poste a tutela dei dati personali sconosciute all'utente
- Rischi di trasferimenti dei dati dell'utente in paesi che non forniscono adeguati livelli di protezione o che permettono c.d. *surveillance programmes*
- **Possibile utilizzo dei dati, da parte del provider, in autonomia e per finalità proprie senza autorizzazione dell'utente**

# *Cosa deve fare l'utente cloud?*

L'adozione di servizi di cloud non esime le imprese e gli studi professionali che se ne avvalgono per la gestione del proprio patrimonio informativo dalle loro responsabilità, in qualità di Titolari del trattamento, dalla disciplina in materia di protezione dei dati personali (D.Lgs. 196/2003 "Codice Privacy")

**In caso di violazioni commesse dal cloud provider, anche il Titolare sarà chiamato a rispondere dell'eventuale illecito.**

*La differenza di velocità tra diritto e tecnologia dimostra come nessuna norma possa tutelarci davvero in assenza di un* ***consapevole esercizio della nostra "autodeterminazione informativa"****, soprattutto sulla protezione dati. («La vita degli altri: controllo e privacy nella società digitale» Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali, 1 ottobre 2014)*



«*Nessuno lascerebbe in deposito il proprio portafoglio con i documenti e lo stipendio alla prima persona incontrata al mercato. La voce "risparmio" non deve quindi essere l'unico fattore di scelta*.» (Vademecum del Garante *Cloud computing: proteggere i dati per non cadere dalle nuvole*)

- La difesa del proprio "patrimonio dati", la trasparenza e la correttezza, contribuiscono a **facilitare i rapporti dell'organizzazione con i clienti** (e tutti gli interessati) e a prevenire eventuali contenziosi
- Particolare attenzione alla modalità con cui si adottano le soluzioni di cloud, affinché le opportunità di efficienza e risparmio non si trasformino in un **rischio per la sicurezza o la disponibilità dei dati**
- Adozione di *best practice* che possono migliorare non solo l'immagine dell'organizzazione, ma anche la **capacità di business a parità di costi** sostenuti, aumentando la fiducia nella sua serietà e affidabilità

# Gli aspetti pratici da valutare

**A** ***Fase pre-contrattuale***:

- Censimento dei **trattamenti e dei dati** (dati personali, comuni, sensibili, etc.)
- Valutazione delle necessità dell'adozione del *cloud* (pro e contro) alla luce delle **concrete esigenze**
- Verifica preliminare dell'**affidabilità** del provider di cloud
- **Individuazione della soluzione di cloud** rispetto alle categorie di dati e trattamenti coinvolti

## B *In sede contrattuale:*

- Valutazione delle **clausole contrattuali** con il provider
- Definizione dei **ruoli privacy** dell'utente e del provider e rispettive attività
- Valutazione dell'**ambito territoriale** di circolazione dei dati
- Valutazione delle **misure di sicurezza** adottate dal provider

# *Quali clausole occorre verificare?*

- ✓ ***Chiara definizione ruoli privacy***: l'utente dovrà accertarsi che il provider sia nominato quale Responsabile del trattamento e che non vi siano **clausole ambigue riguardo la possibilità, per lo stesso, di utilizzare i dati al di fuori delle istruzioni del Titolare** e per proprie finalità (es. di marketing);
- ✓ ***Trasferimenti di dati all'estero***: l'utente deve sapere **in quale Paese risiedono i server di conservazione dei dati**. Per il Codice Privacy infatti i trasferimenti di dati personali in Paesi extra-UE possono avvenire **solo con standard di protezione adeguati a quelli europei** (per es. tramite specifiche Clausole Contrattuali fornite dalla Commissione Europea, mentre **i trasferimenti non potranno più avvenire se il cloud provider USA aderisca al regime c.d. Safe Harbor**, dichiarato invalido dalla Corte di Giustizia Europea lo scorso 6 ottobre). Ciò tenendo conto anche di **normative specifiche** (es. sul trasferimento all'estero della documentazione contabile e divieto di conservazione sostitutiva all'estero per scritture contabili, fatture acquisto, libri sociali obbligatori, DDT);
- ✓ ***Controlli sull'attività del provider***: l'utente come Titolare del trattamento avrà **poteri di supervisione, ispezione e controllo**, con corrispondente obbligo di cooperazione da parte del provider. Tali verifiche potranno essere effettuate da un terzo affidabile (es. anche mediante **certificazione degli standard ISO** recentemente elaborati per i fornitori di servizi di cloud);

- ✓ ***Subappaltatori***: i provider devono informare gli utenti e ottenerne il consenso all'**affidamento di operazioni sui dati a subappaltatori**, descrivendo tali operazioni e **imponendo ad essi gli stessi obblighi assunti dal provider**;
- ✓ ***Conservazione dei dati***: adeguate garanzie dal provider sulla conservazione dei dati al di fuori di quanto esplicitamente stabilito con l'utente, **cancellazione effettiva** dei dati dai mezzi di storage (es. sovrascrittura);
- ✓ ***Cifratura dei dati***: i dati trasmessi devono essere cifrati con standard di algoritmi riconosciuti;
- ✓ ***Tracciamento degli accessi***: rilevamento dei *log* di accesso ai dati personali sul cloud da parte degli operatori del provider e subappaltatori;
- ✓ ***Violazioni dei dati, perdita, alterazione***: verificare la presenza di clausole contrattuali che **pongano a carico del provider** inadempienze, accessi non consentiti, perdita dei dati, indisponibilità per malfunzionamenti, etc. Inoltre, privilegiare contratti che prevedano l'obbligo del fornitore di **notificare eventuali violazioni di dati pe**rsonali all'utente o alle autorità;
- ✓ ***Portabilità dei dati***: consigliabile ricorrere a cloud basati su formati e standard aperti, che facilitino la transizione da un sistema cloud ad un altro, anche se gestiti da fornitori diversi;

- ✓ ***Diritti d'accesso degli interessati***: verificare che il provider non ponga ostacoli tecnici e organizzativi alle richieste d'accesso;
- ✓ ***Assicurazione*** o procedure semplificate per la risoluzione di controversie, anche internazionali, soprattutto per **utenti di piccole dimensioni**.

***…e infine***

- ✓ ***Disponibilità dei dati***: **mantenere copia (es. back-up) dei dati** dalla cui perdita potrebbero conseguire danni economici per l'immagine o attività svolte (es. in caso di servizi di hard-disk remoto, mail, conservazione documentale, etc.)
- ✓ ***Formazione***: specifici **interventi formativi** sul corretto utilizzo del cloud nonché su inserimento e consultazione dei dati, contro eventuali comportamenti sleali o fraudolenti, errori materiali, negligenza;

# Grazie per l’attenzione

**Avv. Daniele Vecchi**

DVecchi@gop.it
www.gop.it

Il presente documento è stato elaborato in modo indipendente da Gianni, Origoni, Grippo, Cappelli & Partners e consegnato a mero scopo informativo, pertanto, a causa dei continui cambiamenti di leggi, norme e regolamenti, potrebbe non essere aggiornato. Le informazioni qui contenute si basano su fonti ritenute attendibili e in buona fede. Tuttavia, non si rilascia nessuna dichiarazione o garanzia, espressa o implicita, né si garantisce l’imparzialità, l’accuratezza, la completezza o la correttezza delle informazioni contenute in questo documento. Questo documento, compresa ogni sua parte, non costituisce un riferimento per contratti o obblighi di alcun tipo, né può costituire in alcun modo una base affidabile per la conclusione di un accordo. Gianni, Origoni, Grippo, Cappelli & Partners non può essere ritenuto responsabile per eventuali danni, diretti o indiretti, derivanti dall’utilizzo del presente documento o del suo contenuto o comunque connessi al suo utilizzo. Il presente documento non può essere riprodotto, distribuito o pubblicato in tutto o in parte, per qualsiasi scopo, senza l’espressa autorizzazione da parte di Gianni, Origoni, Grippo, Cappelli & Partners. Per qualsiasi ulteriore chiarimento si prega di contattare Gianni, Origoni, Grippo, Cappelli & Partners.