

**Misure di Tutela e Aspetti Legali
nel contesto del Cloud Computing**

I dati nella ‘nuvola’: aspetti legali e
contrattuali

Avv. Pierluigi Perri

*Dottore di ricerca in Informatica giuridica e
diritto dell'informatica nell'Università di Bologna*

About me

- Avvocato (privacy, computer crimes, computer forensics, proprietà intellettuale)
- Dottore di ricerca in informatica giuridica e diritto dell'informatica
- Fellow presso l'Università di Stanford
- Ricercatore presso l'Università degli Studi di Milano
- Socio AIPSI e CLUSIT

Il cloud computing per il giurista

- Dal canto nostro, il *cloud computing* si traduce nella condivisione o conservazione, da parte degli utenti, di dati o applicazioni su server di proprietà o gestiti da terzi, ai quali si accede tramite Internet.
- Quello che noi vediamo con preoccupazione, quindi, al di là degli indubbi vantaggi in termini di costi, efficienza, outsourcing della gestione del patrimonio informativo, è questo flusso di dati che viaggia verso “nuvole”.
- Trattandosi di offerte rivolte tanto al privato quanto all’azienda e all’ente governativo, è evidente che molta attenzione deve essere posta agli aspetti di riservatezza dei dati e sicurezza delle informazioni.

Considerazioni e rischi

- L'outsourcing della gestione dei dati, comporta che tali dati saranno affidati, anche per ciò che riguarda la loro riservatezza, a terzi;
- Gli accordi contrattuali e le policy possono variare a seconda del *cloud provider*;
- Alcune leggi prevedono, per determinati soggetti, specifici accordi di riservatezza o segretezza prima di poter affidare informazioni a terzi (vedi HIPAA) o lo vietano (vedi caso della British Columbia) o lo rendono poco consigliabile (conflitto EU-USA per PATRIOT Act);
- I dati possono essere soggetti a *disclosure* qualora i *cloud server* si trovino in un'area geografica con un diverso regime giuridico;
- Possono esserci responsabilità diverse da parte dei titolari del trattamento e diritti diversi per gli interessati;

Considerazioni e rischi/2

- Potrebbe accadere che le informazioni che costituiscono un “dato” siano sparse tra diverse nuvole che rispondono a regimi giuridici differenti;
- La difficoltà di individuare il *locus* del trattamento comporta anche una difficoltà nella definizione delle clausole contrattuali;
- Possibilità di *lock-in* verso uno specifico fornitore;
- Bisogna trovare una soluzione, e tale soluzione passerà necessariamente attraverso tre direttrici:
 - Consapevolezza degli utenti;
 - Predisposizione di contratti con SLAs ben definiti;
 - Cooperazione internazionale per la definizione di un quadro giuridico globale uniforme.

Alcuni esempi

- Professioni che trattano dati che devono essere coperti da segreto (avvocati, medici);
- Rivelazione, da parte del *cloud provider*, di segreti imposta da governi stranieri (cfr. Privacy Commissioner of Canada vs. SWIFT);
- Fallimento di un *cloud provider*;
- Valore economico dei segreti industriali;
- Difficoltà nel reperimento di informazioni per far valere una pretesa in giudizio o esercitare il diritto di difesa;
- Rischi per la propria *business continuity*.

Cosa fare dunque?

Scegliere il *cloud provider* in relazione a specifici parametri che possono essere così riassunti:

- ***Flessibilità*** della proposta commerciale sia in termini di costi sia in termini di servizi possibili;
- ***Livello minimo del servizio*** in relazione alla protezione dei dati e alla continuità;
- ***Trasparenza*** in merito alla logica applicata al trattamento;
- ***Personalizzazione*** della sicurezza lato utente;
- ***Controllo*** del servizio per tutta la durata del rapporto;
- ***Esistenza di una policy pubblica*** del fornitore in merito alla riservatezza dei dati;
- ***Interoperabilità*** della soluzione cloud.

Due diligence del titolare del trattamento

- Per quanto si possa affidare all'esterno della propria struttura un determinato trattamento, il titolare resta comunque responsabile di una generica attività di custodia e controllo delle operazioni di trattamento
- Tale attività, potrà consistere in:
 - Verifica della rispondenza di quanto desumibile dal contratto con il servizio concretamente offerto;
 - Identificazione e immediata segnalazione delle eventuali problematiche;
 - In ragione dei dati trattati, richiesta di reportistica utile a illustrare il pieno rispetto dei parametri inseriti negli SLAs.
 - Utilizzo dei modelli internazionali (ISMS) sia di seconda che terza parte

Problemi di conflitto tra le leggi

- Tipicamente, in uno scenario *cloud*, possono verificarsi due situazioni:
 - Trasferimento di dati all'interno dell'UE;
 - Trasferimento di dati verso Paesi terzi.

Trasferimento di dati verso Paesi appartenenti all'UE

- Siamo tutti “figli” della Direttiva 95/46/CE
- Art. 42. Trasferimenti all'interno dell'Unione europea
 - 1. Le disposizioni del presente codice non possono essere applicate in modo tale da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea, fatta salva l'adozione, in conformità allo stesso codice, di eventuali provvedimenti in caso di trasferimenti di dati effettuati al fine di eludere le medesime disposizioni.

Trasferimento di dati verso Paesi terzi

- Per il nostro Codice, tali trasferimenti sono consentiti solo se:
 - a) l'interessato ha manifestato il proprio consenso espresso o, se si tratta di dati sensibili, in forma scritta;
 - b) è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;
 - e) è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

Oppure...

- Il trasferimento di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è altresì consentito quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato:
 - a) individuate dal Garante anche in relazione a garanzie prestate con un contratto o mediante regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo. L'interessato può far valere i propri diritti nel territorio dello Stato, in base al presente codice, anche in ordine all'inosservanza delle garanzie medesime;
 - b) individuate con le decisioni previste dagli articoli 25, paragrafo 6, e 26, paragrafo 4, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, con le quali la Commissione europea constata che un Paese non appartenente all'Unione europea garantisce un livello di protezione adeguato o che alcune clausole contrattuali offrono garanzie sufficienti.

In una parola: cooperazione internazionale

- Da più parti, si invoca la firma di una Convenzione universale che disciplini il trattamento dei dati da parte di soggetti che offrono servizi tali per cui i dati sono “ubiqui”;
- Il raggiungimento di tale obiettivo può sicuramente essere agevolato da una visione comune di *privacy policy* adottata dai vari *cloud provider*
- Alcuni contatti sono già in essere, quali quelli dell’EU-US High Level Contact Group (cfr. *U.S., EU Issue Statement on Common Data Privacy and Protection Principles*).

Il “modello” Safe Harbour

- Al fine di non ingessare i rapporti commerciali tra USA ed EU, è stato raggiunto l'accordo denominato Safe Harbour;
- Tramite questo accordo, le aziende USA che sottoscrivono determinati principi fondamentali (ad es. rendere l'informativa agli interessati, garantire l'esercizio dei diritti, proteggere le informazioni e garantire la loro integrità) sono autorizzate a trattare dati di soggetti UE;
- Anche in questo caso, l'adesione è facilitata dall'adozione di una *privacy policy* pubblica e dalla predisposizione di un punto di contatto, presso la propria azienda, per le specifiche esigenze di tutela della riservatezza ed esercizio dei diritti da parte degli interessati.

Al momento, però, c'è confusione

- In un'opinione del WP29 di dicembre 2009 (02356/09/en WP 168) si legge che, nonostante la previsione contenuta nell'art. 4 della Direttiva 95/46/CE, non è ancora chiaro se, in caso di diverse sedi di una multinazionale in diversi Stati, si debba applicare una specifica legge e, in caso, quale.
- Attualmente il WP29 sta lavorando ad un documento su questa specifica tematica.

E in Italia

- Art. 5. Oggetto ed ambito di applicazione
 - 1. Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.
 - 2. Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. In caso di applicazione del presente codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali.

Avv. Pierluigi Perri

Email: pierluigi.perri@mpslaw.it

Websites: www.mpslaw.it - www.pierluigiperri.it