

**PROFILI NORMATIVI E CONTRATTUALI RELATIVI
ALLA SICUREZZA E ALLA RISERVATEZZA DEI DATI
NEI SERVIZI DI CLOUD COMPUTING**

Avv. Giorgio Spedicato



Come evolve il business nell'era del Cloud Computing

Giovedì 27 Gennaio 2011

CHI SONO

Managing Partner dello studio legale Monducci Perri Spedicato & Partners.

Dottore di ricerca in Informatica giuridica e diritto dell'informatica.
Docente di Diritto della Proprietà intellettuale presso la Facoltà di Giurisprudenza dell'Università di Bologna (polo didattico di Ravenna).

CHI È MPS

Lo Studio legale associato Monducci Perri Spedicato & Partners è una *law boutique* specializzata in proprietà intellettuale, diritto delle nuove tecnologie e diritto dell'innovazione.

Affianca chi fa dell'innovazione il proprio lavoro e il proprio impegno quotidiani, supportandolo nell'attività *day by day* e assistendolo nelle operazioni più complesse.

A PROPOSITO DI CLOUD COMPUTING...

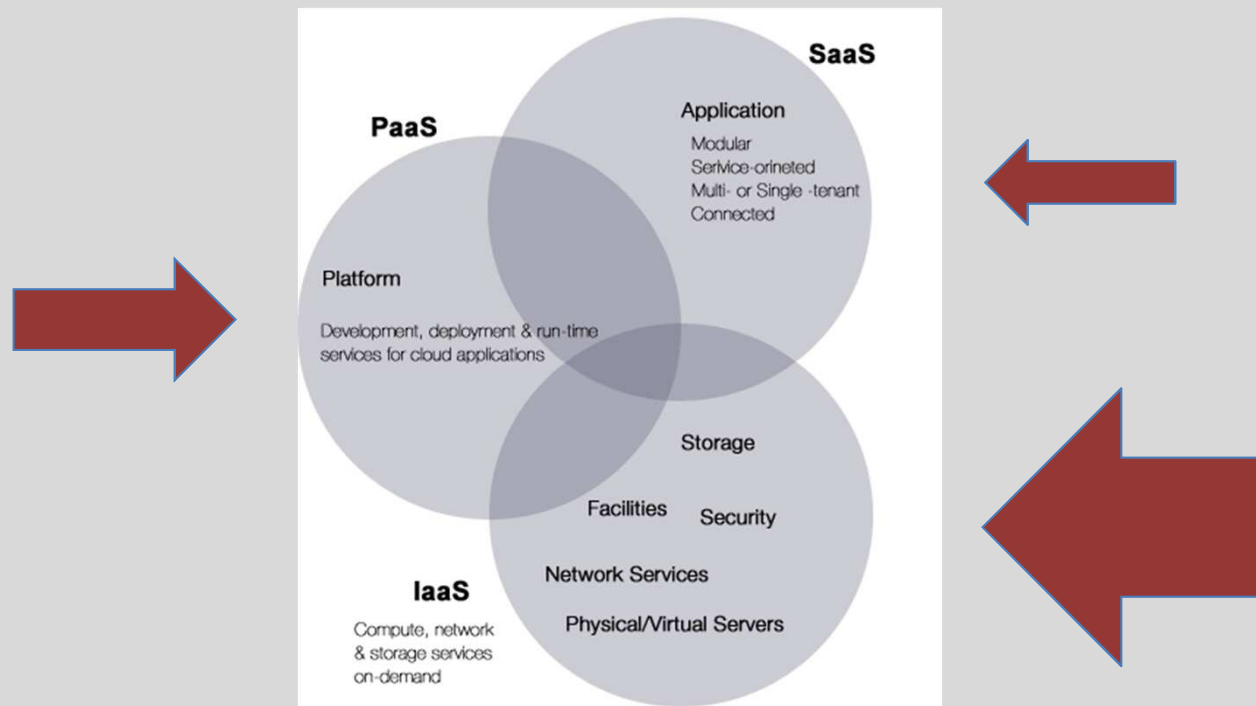
«One reason you should not use web applications to do your computing is that **you lose control**. It's just as bad as using a proprietary program. Do your own computing on your own computer with your copy of a freedom-respecting program. If you use a proprietary program or somebody else's web server, you're defenseless. You're putty in the hands of whoever developed that software»

(Richard Stallman)

«Occorre riflettere anche sui rischi che pone la nuova tecnologia del "cloud computing", con la quale **i dati verranno sempre più sottratti alla disponibilità materiale di chi li produce e usa**, e gestiti da enormi server collocati in ogni parte del pianeta»

(Francesco Pizzetti)

PERDITA DI CONTROLLO SUI DATI



«WWW» NON È SOLO «WORLD WIDE WEB»...

La perdita di controllo sui dati è relativa al:

- CHI può accedere ai dati (**WHO**)
- COSA viene fatto con i dati (**WHAT**)
- DOVE si trovano i dati (**WHERE**)

ALCUNI PROBLEMI LEGALI DERIVANTI DALLA PERDITA DI CONTROLLO SUI DATI

- ✓ Quale legge è applicabile al contratto?
- ✓ Qual è il foro competente?
- ✓ Come garantire la titolarità dei dati?
- ✓ Come garantire la salvaguardia dei segreti aziendali?
- ✓ Come garantire la possibilità di acquisizione forense di prove digitali?
- ✓ Come garantire la *legal compliance* in relazione al trattamento dei dati personali?
- ✓ Come garantire la massima sicurezza nel trattamento dei dati?
- ✓ Etc...

LA TUTELA DEI DATI PERSONALI NELLA «NUVOLA»: ALCUNI PROFILI CRITICI

- ✓ Applicabilità del d.lgs. 196/2003 al *cloud provider*
- ✓ Ruolo del *cloud provider* nel trattamento dei dati
- ✓ Trasferimento dei dati all'estero

APPLICABILITÀ DEL D.LGS. 196/2003 AL CLOUD PROVIDER

È possibile applicare il Codice al *cloud provider* quando quest'ultimo:

- ✓ è stabilito in Italia (art. 5, co. 1);
- ✓ è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, **strumenti situati in Italia** anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea (art. 5, co. 2).



Se il *cloud provider* ha la propria sede e le proprie infrastrutture al di fuori del territorio dello Stato non potrà essere assoggettato al Codice

RUOLO DEL CLOUD PROVIDER NEL TRATTAMENTO DEI DATI

CONTITOLARE O RESPONSABILE DEL TRATTAMENTO?

- ❑ Il **TITOLARE** del trattamento è la «persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le **decisioni** in ordine alle **finalità**, alle **modalità** del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della **sicurezza**» (art. 4, co. 1, lett. f).
- ❑ Il **RESPONSABILE** del trattamento è la «persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo **preposti dal titolare** al trattamento di dati personali» (art. 4, co. 1, lett. g).

RUOLO DEL CLOUD PROVIDER NEL TRATTAMENTO DEI DATI

L'art. 29, d.lgs. 196/2003, pone qualche problema applicativo...

«Il responsabile è designato dal titolare facoltativamente.

Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite **verifiche periodiche**, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni».

TRASFERIMENTO DEI DATI ALL'ESTERO

Art. 43, d.lgs. 196/2003

1. Il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, se diretto verso un Paese non appartenente all'Unione europea è consentito quando:

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;

(...)

h) il trattamento concerne dati riguardanti persone giuridiche, enti o associazioni.

TRASFERIMENTO DEI DATI ALL'ESTERO

Art. 44, d.lgs. 196/2003

«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;
- 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.

TRASFERIMENTO DEI DATI ALL'ESTERO

Art. 45, d.lgs. 196/2003

«Fuori dei casi di cui agli articoli 43 e 44, il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è **vietato quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato**. Sono valutate anche le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza».

TRASFERIMENTO DEI DATI ALL'ESTERO

In conclusione, per effettuare un trasferimento di dati all'estero, è possibile seguire una delle seguenti strade:

- ✓ **Trasferimento di dati verso i soli Paesi che offrono garanzie adeguate:** ad oggi si tratta di (Svizzera, Canada, Argentina, Isola di Guernsey, Isola di Man, Isola di Jersey, Isole Far Oer, Andorra, USA limitatamente alle imprese che aderiscono al c.d. *Safe Harbor*)
- ✓ Inserimento nel contratto delle **clausole contrattuali standard approvate dalla Commissione** europea (cfr. da ultimo le decisioni della Commissione europea 2004/915/CE e 2010/87/UE)
- ✓ Previsione di *binding corporate rules* (applicabili tuttavia solo ai trasferimenti di dati all'interno di gruppi di società)
- ✓ **Consenso espresso** dell'interessato *ex art. 43 del Codice*

ALCUNI PROFILI CRITICI RELATIVI ALLA SICUREZZA DEI DATI NELLA «NUVOLA»

❑ I RISCHI CONNESSI ALL'ACCESSO AI DATI

«Before, the bad guys usually needed to get their hands on people's computers to see their secrets; in today's cloud all you need is a password»

(Jonathan Zittrain)

- ✓ da parte di *crackers*
- ✓ da parte di concorrenti
- ✓ da parte di autorità pubbliche
- ✓ da parte dello stesso provider o di suoi dipendenti infedeli

ALCUNI PROFILI CRITICI RELATIVI ALLA SICUREZZA DEI DATI NELLA «NUVOLA»

I RISCHI CONNESSI ALLA **CONSERVAZIONE** DEI DATI

- ✓ come garantirsi che i dati siano sempre recuperabili e che essi non vengano corrotti?
- ✓ come garantirsi in caso di fallimento del *cloud provider*?

I RISCHI CONNESSI ALLA **CANCELLAZIONE** DEI DATI

- ✓ alcune norme prevedono la cancellazione di determinate categorie di dati decorso un certo periodo di tempo dalla loro raccolta;
- ✓ in altri casi il titolare potrebbe avere interesse a cancellare in modo definitivo, per svariate ragioni, alcuni dati
- ✓ come accertarsi che i dati che il titolare deve/vuole cancellare non siano più recuperabili?

RIACQUISIRE IL CONTROLLO...ATTRAVERSO IL CONTRATTO

La *best practice* in relazione all'acquisizione di servizi *cloud* da parte di un'impresa impone, da un punto di vista legale:

- ✓ di preferire *cloud provider* che siano disposti a negoziare le condizioni contrattuali del servizio;
- ✓ preferire *cloud provider* i cui *data center* siano in un Paese dell'UE (e.g. Amazon S3)
- ✓ di preferire *cloud provider* che offrano adeguate garanzie in termini patrimoniali;
- ✓ di preferire *cloud provider* che offrano adeguate garanzie in termini tecnici;
- ✓ di preferire *cloud provider* che offrano adeguate garanzie in termini di trasparenza.

RIACQUISIRE IL CONTROLLO...ATTRAVERSO IL CONTRATTO

Clausole su cui è opportuno negoziare (o focalizzare la propria attenzione per l'ipotesi in cui non sia possibile negoziare) :

- ✓ clausole relative alla titolarità dei dati
- ✓ clausole di *data export*
- ✓ clausole relative al rispetto della normativa privacy in relazione al trattamento dei dati
- ✓ clausole relative agli SLA
- ✓ clausole relative alle misure di sicurezza adottate nel trattamento dei dati
- ✓ clausole di audit
- ✓ clausole relative al *back up* e alla *recovery* dei dati
- ✓ clausole di responsabilità per la perdita o l'accesso non autorizzato ai dati
- ✓ clausole relative alla *termination* del contratto
- ✓ clausole relative a legge applicabile e foro competente

STUDIO LEGALE ASSOCIATO

MILANO

Via Larga, 6
20122 Milano
Tel. 02.89926248
Email: milano.desk@mpslaw.it

BOLOGNA

Via dell'Indipendenza, 36
40121 Bologna
Tel. 051.7878043
Email: bologna.desk@mpslaw.it

IMOLA

Via Garibaldi, 40
40026 Imola (Bo)
Tel. 0542.30702
Email: imola.desk@mpslaw.it

GRAZIE DELL'ATTENZIONE!

Avv. Giorgio Spedicato

email: giorgio.spedicato@mpslaw.it

skype: [giorgio.spedicato](https://www.skype.com/people/giorgio.spedicato)

MONDUCCI PERRI SPEDICATO & PARTNERS

www.mpslaw.it