Studio Legale
Alberto Savi & Associati

MIP
POLITECNICO DI MILANO
SCHOOL OF MANAGEMENT

Profili legali e contrattuali nei servizi di cloud computing

Anna Italiano
Avvocato

Il Cloud computing dal punto di vista legale

Mancanza di un quadro normativo organico e specifico

Potenziali rischi di compliance normativa

Il ricorso a forme di esternalizzazione non può essere inteso come «deresponsabilizzazione»

I principali rischi connessi all'adozione dei servizi di cloud computing

- Perdita del controllo diretto ed esclusivo sui dati di propria titolarità.
- Spesso il servizio prescelto viene fornito attraverso le prestazioni di subfornitori diversi da quelli con cui l'utente stipula il contratto.
- La disponibilità dei dati allocati nella nuvola non è incondizionatamente garantita.
- L'utente non sempre è messo in grado di conoscere l'ubicazione dei data center.
- Rischio di vendor lock-in.
- Rischi per la confidenzialità e la riservatezza dei dati.

Fonti normative

- Codice Privacy italiano (d. lgs. 196/2003)
- Direttiva 95/46/CE sul trattamento e la protezione dei dati personali
- Direttiva e-privacy 2002/58/CE (modificata dalla direttiva 2009/136/CE), che si applica al trattamento dei dati personali nel settore delle comunicazioni elettroniche
- Nuovo Regolamento UE in materia di dati personali (in corso di approvazione)

Spunti di interesse provenienti da studi in ambito privacy

- Gruppo di lavoro ex art. 29, Parere 05/2012 - Cloud Computing
- La mini guida del Garante del giugno 2012 :“Proteggere i dati per non cadere dalle nuvole”
- Commission expert group

Ripartizione di ruoli e responsabilità tra i diversi attori

Art. 4 Codice Privacy

Titolare

«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».

Responsabile

«La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali».

Interessato

«la persona fisica cui si riferiscono i dati personali».

IL CLIENTE CLOUD

*"**Il cliente cloud determina la finalità ultima del trattamento** e decide in merito all'esternalizzazione di tale trattamento e alla delega ad un'organizzazione esterna delle attività di trattamento, in tutto o in parte"* (WP 29, Opinion 5/2012).

Il cliente cloud agisce, pertanto, in qualità di titolare del trattamento.

Il cliente cloud, in quanto titolare del trattamento, è tenuto all'osservanza di **tutti gli obblighi di legge sulla protezione dei dati personali di cui alla direttiva 95/46/CE e al Codice Privacy italiano.**

"Il cliente cloud può incaricare il fornitore cloud di scegliere I metodi** e le **misure tecniche e organizzative da utilizzare per conseguire gli scopi del responsabile del trattamento". (WP 29, Opinion 5/2012).

IL FORNITORE CLOUD

Il fornitore cloud è colui fornisce i servizi di cloud computing.

Quando fornisce gli strumenti e la piattaforma, agendo per conto del cliente cloud, **il fornitore cloud è considerato alla stregua di un responsabile del trattamento**

I fornitori di servizi di cloud computing, in quanto responsabili del trattamento, hanno il dovere di **garantire la riservatezza dei dati** e **sono responsabili dell'adozione di misure di sicurezza**, in linea con quanto previsto dalla normativa UE e dalla legislazione nazionale.

La mini guida del Garante del giugno 2012 "Proteggere i dati per non cadere dalle nuvole

Le indicazioni del Garante sul riparto degli obblighi tra le parti del trattamento

- **La pubblica amministrazione o l'azienda, "titolare del trattamento" dei dati personali, che trasferisce del tutto o in parte il trattamento di dati personali a un fornitore, deve procedere a designare il fornitore dei servizi cloud "responsabile del trattamento"**

- **In caso di violazioni commesse dal fornitore** (o da un subfornitore), **anche il titolare sarà chiamato a rispondere dell'eventuale illecito**. Non sarà sufficiente per giustificare una eventuale violazione affermare di non avere avuto possibilità di negoziare clausole contrattuali o modalità di controllo stringenti: **il cliente di servizi cloud 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**, verificando la corretta esecuzione delle istruzioni impartite in relazione ai dati personali trattati

La mini guida del Garante del giugno 2012 "Proteggere i dati per non cadere dalle nuvole

Le indicazioni del Garante sul riparto degli obblighi tra le parti del trattamento

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
- **Il titolare del trattamento dovrà quindi tenere in debito conto anche il luogo dove vengono conservati i dati e quali sono i trattamenti previsti all'estero**

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
- **Occorre quindi contrattualmente imporre ai fornitori non solo il rispetto delle misure minime di sicurezza previste dall'allegato B al d.lgs 196/03 ma anche un livello di sicurezza che, di volta in volta in considerazione delle caratteristiche di ogni contratto, possa essere ritenuto idoneo**

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

La mini guida del Garante del giugno 2012
"Proteggere i dati per non cadere dalle nuvole

Scegliere un cloud provider di qualità: i consigli operativi del Garante
Il Garante consiglia di fare una valutazione dei rischi, costi e benefici preventiva rispetto all'utilizzo di servizi cloud.
Valutare il **tipo di cloud** e il **modello di servizio** più adatti alle proprie esigenze ed al **tipo di dati** che si ha la necessità di esternalizzare.
La voce «risparmio» non deve essere l'unico fattore di scelta.
Sfruttare l'ampiezza del mercato, scegliendo tra differenti provider.
Il decalogo per valutare l'impatto dei servizi cloud sull'impresa o sulla PA

La mini guida del Garante del giugno 2012
"Proteggere i dati per non cadere dalle nuvole

Il decalogo del Garante

Effettuare una verifica sull'affidabilità del fornitore

Gli utenti dovrebbero accertare e valutare:
l'esperienza, la capacità e l'affidabilità del fornitore;
- la struttura societaria del fornitore, le referenze, le garanzie di legge offerte in ordine alla confidenzialità dei dati e alle misure adottate per assicurare la continuità operativa a fronte di eventuali e imprevisti malfunzionamenti;
- Gli utenti dovrebbero valutare, inoltre, le **caratteristiche qualitative dei servizi di connettività di cui si avvale il fornitore in termini di capacità e affidabilità;**
- Il cliente deve valutare **l'impiego da parte del fornitore di personale qualificato, l'adeguatezza delle sue infrastrutture informatiche e di comunicazione, la disponibilità ad assumersi una responsabilità risarcitoria in caso di eventuali falle nel sistema di sicurezza o di interruzioni del servizio**

Importanza delle certificazioni indipendenti (es. ISO)

La mini guida del Garante del giugno 2012 "Proteggere i dati per non cadere dalle nuvole

Il decalogo del Garante

Privilegiare i servizi che favoriscono l'interoperabilità e la portabilità dei dati

In particolare, è consigliabile ricorrere a servizi di cloud computing privilegiando quelli basati su formati e standard aperti, che facilitino la transizione da un sistema cloud ad un altro, anche se gestiti da fornitori diversi.

Assicurarsi la disponibilità dei dati in caso di necessità (continuità operativa e disaster recovery)

È opportuno chiedere che nel contratto con il fornitore siano ben specificate adeguate garanzie sulla disponibilità e sulle prestazioni dei servizi cloud.

L'importanza degli SLA

La mini guida del Garante del giugno 2012
"Proteggere i dati per non cadere dalle nuvole

Il decalogo del Garante

Selezionare i dati da inserire nella nuvola

Non perdere di vita di dati

È sempre opportuno che l'utente valuti accuratamente il tipo di servizio offerto, anche **verificando se i dati rimarranno nella disponibilità fisica dell'operatore con cui è stato stipulato il contratto oppure se questi svolga un ruolo di intermediario**, ovvero offra un servizio basato sulle tecnologie messe a disposizione da un operatore terzo.

L'importanza della trasparenza sulla lista dei sub contractor

Informarsi su dove risiederanno concretamente i dati

È importante per l'utente sapere se i propri dati vengono trasferiti ed elaborati da server in Italia, in Europa o in un Paese extraeuropeo.

Giurisdizione e legge applicabile

Livello di protezione assicurato ai dati trasferiti

La mini guida del Garante del giugno 2012 "Proteggere i dati per non cadere dalle nuvole

Il decalogo del Garante

Porre attenzione alla clausole contrattuali

È importante valutare l'idoneità delle condizioni contrattuali per l'erogazione del servizio di cloud con particolare riferimento:

- agli **obblighi e alle responsabilità in caso di perdita, distruzione o illecita diffusione dei dati** custoditi nella nuvola;
- alle modalità di esercizio del **diritto di recesso**;
- alla possibilità di **migrare ad altro fornitore;**
- alla previsione di **livelli di servizio e relative penali** per l'ipotesi di violazione;
- al **trattamento dei dati**, e specificamente:
  - **accesso ai dati** e **clausola di riservatezza;**
  - **Logging ed auditing del trattamento**;
  - **Misure tecniche ed organizzative** volte a garantire la **disponibilità, l'integrità e la riservatezza dei dati**;
- al **subappalto,** e in particolare:
  - previo consenso al subappalto da parte del titolare del trattamento;
  - obbligo di informare il titolare dell'eventuale modifica dei subappaltatori, a fronte del diritto del titolare di opporsi o risolvere il contratto;
  - responsabilità del fornitore per le violazioni poste in essere dai propri subappaltatori.

La mini guida del Garante del giugno 2012
"Proteggere i dati per non cadere dalle nuvole

Il decalogo del Garante

Verificare il rispetto delle finalità, dei tempi e delle modalità di conservazione dei dati

In fase di acquisizione del servizio cloud è opportuno approfondire e prevedere nel contratto le politiche adottate dal fornitore riguardo a:

- tempi di conservazione dei dati;
- modalità di cancellazione.

Esigere adeguate misure di sicurezza

In generale si raccomanda di privilegiare i fornitori che utilizzino **modalità di archiviazione e trasmissione sicure, mediante tecniche crittografiche** (specialmente quando i dati trattati sono particolarmente delicati), accompagnate da **robusti meccanismi di identificazione dei soggetti autorizzati all'accesso.**

Formare adeguatamente il personale

Il personale, sia quello del cliente che quello del fornitore, incaricato del trattamento dei dati mediante servizi di cloud computing dovrebbe essere appositamente formato, al fine di limitare rischi di accesso illecito, di perdita di dati o, più in generale, di trattamento non consentito.

Quali interrogativi porsi (e porre ai fornitori)	Esigenze minime di tutela
Quali sono le **misure di sicurezza adottate dal fornitore** per proteggere i dati? È possibile che i **dati sul cloud possano essere persi o distrutti**?	Adozione di adeguate misure di sicurezza e sistemi di logging
In caso di problemi al collegamento Internet, è comunque possibile continuare a usufruire dei servizi senza l'accesso al cloud? **In quanto tempo può essere ripristinato il sistema**? Esistono piani di emergenza per i servizi essenziali?	Piani di emergenza, continuità operativa, disaster recovery
Chi è il **reale fornitore del servizio che si sta acquisendo**? Si tratta di una singola società o di un consorzio di imprese?	Trasparenza sulla catena dei subfornitori
In quale Stato sono conservati i dati caricati sulla "nuvola"? È possibile scegliere di usufruire di server collocati solo in territorio nazionale o in Paesi dell'Unione europea?	Adempimenti relativi al flusso transfrontaliero dei dati
La tecnologia utilizzata dal fornitore di cloud è di tipo "**proprietario**"? **I dati possono essere esportati facilmente?**	Interoperabilità, portabilità, no lock-in dei dati
Esistono **garanzie di riservatezza** per i nostri dati nel caso in cui un concorrente condivida gli stessi servizi cloud?	Clausole di riservatezza
Nel caso in cui si accerti una violazione o la perdita dei dati, **il fornitore garantisce un pronto risarcimento del danno**?	Attenta valutazione delle clausole contrattuali

Grazie per l'attenzione!

Per domande ed approfondimenti:

annamaria.italiano@studioisl.it