Sicurezza dei dati e delle informazioni all'epoca del cloud
Le norme

15° Meeting nazionale ACEF
Bologna, 30 ottobre 2015

Claudia Cevenini

La nuvola informatica

Insieme di tecnologie che permettono di memorizzare, archiviare, elaborare, trasmettere grandi quantità di dati mediante l'uso di **risorse hardware e software distribuite e virtualizzate in rete**.

I **dati** sono trattati da **fornitori di servizi cloud** e sono conservati presso le loro **server farm**, in Italia o all'estero.

Dati e servizi sono erogati **via Internet** e accessibili da qualsiasi dispositivo (pc, tablet, smartphone), su richiesta dell'utente.

Quale disciplina giuridica?

Se sono trattati **dati personali** in cloud, occorre capire quali regole si debbano applicare.

Il **Codice privacy** italiano (D.Lgs. 196/03) si applica a:

- soggetti stabiliti nello Stato, anche se i dati sono detenuti all'estero;
- soggetti stabiliti fuori dalla UE se utilizzano strumenti ubicati nel territorio dello Stato.

Il Titolare italiano sarà quindi soggetto agli obblighi e alle responsabilità del Codice ovunque si trovino i dati la cui gestione è stata affidata in *outsourcing* al cloud provider.

Evoluzione normativa

E’ in discussione un Regolamento europeo sulla protezione dei dati personali, che sarà direttamente applicabile negli Stati Membri (Regolamento Generale sulla protezione dei dati).

I principi fondamentali resteranno gli stessi ma alcune regole cambieranno, per adeguare la normativa all’evoluzione tecnologica (la Direttiva UE risale al 1995).

La proposta di Regolamento è disponibile on-line: http://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52012PC0011

Ambito di applicazione: cosa cambia

La bozza di Regolamento europeo prevede un diverso «Campo di applicazione territoriale»:

Il Regolamento si applica ai soggetti extra-UE che trattano dati di residenti nell'Unione se il trattamento riguarda:

- l'offerta di beni o la prestazione di servizi ai suddetti residenti, o
- il controllo del loro comportamento.

Ruoli e responsabilità

Impresa o professionista che tratta dati personali agisce come **Titolare**: decide finalità e modalità del trattamento, gli strumenti utilizzati, oltre al profilo della sicurezza.

Il Titolare che tratta dati personali in cloud deve designare il **cloud provider** come **Responsabile** del trattamento.

Il Titolare ha l'obbligo di impartire istruzioni scritte analitiche al Responsabile.

Il Responsabile è tenuto ad attenersi alle disposizioni del Titolare. E' preposto dal Titolare al trattamento di dati personali; non agisce di iniziativa propria ma opera sotto la direzione e la vigilanza del Titolare.

Minacce per la sicurezza dei dati

Cloud – aumento dell'uso di Internet e applicazioni remote, condivisione dei dati, uso di ambienti di collaborazione.

Rischi – accesso non consentito ai dati, sottrazione, distruzione, modifica non autorizzata, trattamento non conforme alle finalità, ecc.

Minacce interne – intenzionali o casuali. Importante adottare misure tecniche e organizzative di sicurezza, istruire adeguatamente gli incaricati del trattamento.

Minacce esterne – accesso abusivo e altri possibili reati informatici, spionaggio industriale.

Rischi per il Titolare 1/2

Diminuzione del controllo sui propri dati e sui trattamenti gestiti dal provider.

Aumento di esposizione dei dati critici, dovuto alle caratteristiche di condivisione del cloud.

Aumento dell'utilizzo di reti pubbliche per l'accesso alle risorse remote.

Rischi per il Titolare 2/2

Il cloud provider potrebbe accedere a dati personali dell'utente o di cui l'utente è Titolare.

Luogo di memorizzazione dei dati non può essere definito a priori e può variare per esigenze operative (es. trasferimento di dati all'estero).

Il cloud provider può avvalersi a sua volta dei servizi cloud di un altro provider (es. un provider SaaS può avvalersi di un provider IaaS) = catena di cloud.

Sicurezza dei dati e dei sistemi 1/2

Disciplinare tecnico in materia di misure MINIME di sicurezza (Allegato B al Codice)

I titolari del trattamento, nel rispetto degli obblighi generali di sicurezza, devono adottare le **misure minime di sicurezza** previste dalla **legge**.

Es: Sistema di autenticazione informatica; profili di autorizzazione; antivirus; aggiornamento periodico dei programmi; backup, ecc.

Sicurezza dei dati e dei sistemi 2/2

Misure c.d. IDONEE

Nel custodire e controllare i dati devono essere adottate **idonee** e **preventive misure di sicurezza** per **ridurre** al **minimo** i **rischi** di **distruzione** o **perdita** (anche accidentale) dei dati, **accesso non autorizzato**, **trattamento non consentito** o **non conforme** agli **scopi**.

Nel predisporre le misure di sicurezza occorre tenere conto di: **progresso tecnico**, **natura dei dati**, **caratteristiche del trattamento**.

Cosa fare?

Gestione delle identità e dei ruoli (Titolare, Responsabile, Incaricati), definizione di privilegi e autorizzazioni.

Attenzione alle utenze admin: è necessario operare in conformità alle prescrizioni del Garante sugli amministratori di sistema.

Gestione del contratto – verificare che il contratto garantisca la conformità effettiva alle norme vigenti.

Contratti di cloud - Legge applicabile

Perdita di controllo fisico – controllo indiretto mediante gli strumenti conferiti all'utente dal contratto.

Tale controllo risulta più difficile se la legge applicabile al contratto o il foro competente è straniero.

Importante sapere se un eventuale provvedimento del giudice (italiano o straniero) verrà eseguito in tempi rapidi.

Occorre verificare che il cloud provider indichi in quale Paese si trovano i data center che ospitano i dati.

Contratti di cloud - Misure di sicurezza 1/3

Occorre verificare che il cloud provider si impegni a rispettare le misure di sicurezza previste dal Codice Privacy.

Non sono sufficienti generiche clausole in cui si impegna a operare in conformità alla normativa vigente.

Opportuno avvalersi di fornitori che indichino dettagliatamente le misure adottate per garantire sicurezza, riservatezza e integrità dei dati.

Contratti di cloud - Misure di sicurezza 2/3

Se il provider è extra-UE potrebbe non essere assoggettato al Codice privacy (lo sarebbe solo in caso di utilizzo di strumenti localizzati in Italia).

Se l'utente Titolare del trattamento è un'impresa o professionista con sede in Italia sarà invece in ogni caso tenuto a rispettare il Codice privacy: dovrà tutelarsi mediante il contratto.

L'utente dovrà esigere dal provider garanzie contrattuali che garantiscano che il servizio fornito e i trattamenti di dati personali nella nuvola siano compatibili con il Codice privacy.

Contratti di cloud - Misure di sicurezza 3/3

Allegato B Misure "minime" di sicurezza: si può prevedere il rilascio di una dichiarazione liberatoria sul rispetto della normativa da parte del fornitore/provider.

Il provider sarà tenuto a garantire il rispetto del Codice privacy solo se soggetto alla legge italiana.

In caso contrario, il Titolare può cercare di ottenere tale garanzia come impegno contrattuale.

Catene di cloud

Dal punto di vista legale, contrattuale e di gestione dei rischi occorre valutare l'aspetto della catena di fornitori (es. provider che si avvale dei servizi di altro provider in cloud).

L'utente potrebbe anche non sapere che il suo fornitore di servizi si appoggia ad altro fornitore in cloud e quindi usare servizi cloud – con tutte le conseguenti problematiche legali – a sua insaputa.

Il Codice privacy non prevede che un Responsabile del trattamento possa designare un altro Responsabile. Il Titolare/cliente dovrebbe vincolare il provider ad appoggiarsi a fornitori che accettino di essere designati a loro volta come Responsabili direttamente dal Titolare.

Contratti di cloud - Luogo del trattamento dei dati

Importante che sia individuato il luogo di trattamento dei dati.

I dati potrebbero trovarsi in Italia, nella UE o in paesi extra-UE.

Nel caso di trasferimento di dati **verso altri paesi UE** non si pongono particolari problemi, in quanto la **circolazione** è **libera**.

Nel caso di trasferimento dei dati extra UE, occorre verificare che siano rispettate le regole per il **corretto trasferimento di dati extra UE** previste dal **Codice privacy**.

Trasferimento di dati all'estero 1/3

All'interno della UE

Il **Codice non può** essere applicato in modo da **limitare** la **libera circolazione** di **dati personali** all'interno dell'Unione Europea.

Possono essere adottati **provvedimenti** se il **trasferimento** di dati all'estero ha lo **scopo** di **eludere** le disposizioni del **Codice**.

Trasferimento di dati all'estero 2/3

Verso Paesi terzi (=extra UE) il trasferimento di dati, anche temporaneo, è possibile se:

- **consenso espresso** dell'interessato (manifestato per **iscritto** se dati sensibili);
- t. necessario per eseguire **obblighi di un contratto** di cui è **parte** l'interessato, adempiere a **richieste** dell'interessato, per concludere o eseguire un **contratto a favore** dell'interessato;
- t. necessario per salvaguardia di un **interesse pubblico** individuato per legge o regolamento;
- t. necessario per salvaguardia della **vita** o **incolumità fisica** di un **terzo**;

Trasferimento di dati all'estero 3/3

- t. necessario per **investigazioni difensive** o per **tutelare** un diritto in **giudizio**;
- t. effettuato in seguito a richiesta di **accesso** a **documenti amministrativi** o di estrazione di dati da **pubblichi elenchi**, registri, ecc. conoscibili da chiunque;
- t. necessario per scopi **storici**, **statistici** o **scientifici**;
- t. riguarda dati di **persone giuridiche**, **enti** o **associazioni**.

Inoltre, **t.** è possibile con l'**autorizzazione** del **Garante** sulla base di adeguate garanzie per i diritti dell'interessato.

Trasferimenti extra UE vietati

Tranne nei casi consentiti di cui agli **artt. 43 e 44**, il **trasferimento anche temporaneo** fuori dal territorio dello Stato, con qualsiasi mezzo e in qualsiasi forma, di **dati personali** verso un **Paese extra UE** è **vietato** quando l'**ordinamento del Paese di destinazione o di transito dei dati non assicura un adeguato livello di tutela delle persone**.

Sono valutate anche le modalità di trasferimento e dei trattamenti previsti, le finalità, la natura dei dati e le misure di sicurezza adottate.

US-EU Safe Harbor

Si **trattava** di un procedimento che le società statunitensi potevano seguire per essere conformi alla normativa europea sulla protezione dei dati personali.

Lo US Department of Commerce aveva sviluppato tale procedimento in collaborazione con l'Unione Europea e la Commissione europea, che lo avevano dichiarato conforme alla normativa UE sulla protezione dei dati personali.

Grazie al SH, era possibile trasferire dati personali verso le imprese statunitensi che vi avevano aderito, in quanto si riteneva garantisse un adeguato livello di tutela.

Il SH è stato recentemente giudicato **illegittimo**.

Cosa è successo e cosa significa?

Il 6 ottobre la **Corte di Giustizia dell'Unione europea** ha emesso una sentenza che stabilisce un principio rilevante per il cloud, nel caso i server siano ubicati negli USA: gli **Stati Uniti non offrono un adeguato livello di tutela** nella protezione dei dati personali.

Maximillian Schrems vs. Data Protection Commissioner. Causa C-362/14.

http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=req&docid=169195&occ=first&dir=&cid=663265

Dopo la sentenza

15 ottobre - Autorità Garanti europee (c.d. Art. 29): "Se non saranno trovate soluzioni appropriate entro la fine del gennaio 2016 le Autorità intraprenderanno ogni azione necessaria e appropriata, incluse eventuali iniziative coordinate di *enforcement*".

26 ottobre - Vera Jourova, Commissaria UE alla Giustizia: "Esiste un accordo di principio con gli Stati Uniti in materia di Safe harbour, ma stiamo ancora discutendo per fare in modo che gli impegni soddisfino appieno le richieste della Corte".

Conclusioni 1/2

Imprese e professionisti devono innanzitutto effettuare un'**attenta verifica** della **conformità** al Codice privacy all'**interno** della propria organizzazione/del proprio studio.

Particolare attenzione dovrà essere dedicata non solo ai noti aspetti formali (informativa, consenso) ma anche alle **misure** di sicurezza **tecniche** e **organizzative idonee** che è opportuno adottare in relazione ai dati personali trattati.

Se intendono utilizzare servizi in cloud, occorre **verificare** le **clausole contrattuali** con la massima attenzione per comprendere se l'adesione al contratto possa comportare rischi o responsabilità, in particolare se il cloud provider non fornisce adeguate garanzie o se è soggetto a un ordinamento giuridico extra-europeo.

Conclusioni 2/2

E’ importante che imprese e professionisti restino **costantemente aggiornati** sull’**evoluzione normativa** in materia di protezione dei dati personali.

Spesso la gestione della ‘privacy’ è affidata a soggetti esterni, con competenze tecniche e non giuridiche.

Ogni impresa, ogni studio necessita di un’analisi personalizzata e non può semplicemente affidarsi a moduli pre-compilati e a software generici.

Grazie per l'attenzione!

Claudia Cevenini
claudia.cevenini@studiocevenini.it