Società Italiana
Telemedicina @ Sanità Elettronica

ORDINE AVVOCATI DI ROMA

Convegno di studio su Privacy e Telemedicina

“Tra diritto del paziente alla riservatezza ed utilità della condivisione del dato sanitario”

CLOUD COMPUTING *IN SANITÀ*

MICHELE MARTONI

Avvocato, Professore a contratto di Informatica giuridica

(Università di Bologna)

Roma, 21 ottobre 2014

Sala Conferenze di Piazza Monte Citorio, 123/a

Paradigma tecnologico

- **Cloud Computing**
  - *Consiste in una serie di tecnologie e modelli di servizio incentrati sull'uso e sulla **fornitura di applicazioni informatiche**, **capacità di elaborazione** e **archiviazione** e **spazio di memoria** basati su Internet*
    - Maggiore facilità nell'accesso alle risorse informatiche
    - Tecnologia più aggiornata (e sicura) a disposizione
    - Costi contenuti in quanto le risorse messe a disposizione possono essere condivise da altri soggetti con le medesime esigenze

Private / Public Cloud

- **Private** *Cloud*
  - è un'infrastruttura informatica dedicata alle esigenze di una singola organizzazione, ubicata nei suoi locali o affidata in gestione ad un terzo nei confronti del quale il Titolare del trattamento esercita un controllo puntuale
- **Public** *Cloud*
  - l'infrastruttura è di proprietà di un fornitore specializzato nell'erogazione di servizi che mette a disposizione di utenti, aziende o pubbliche amministrazioni

Modelli di erogazione dei servizi

- **IaaS** (**Infrastructure** as a Service)
  - il fornitore noleggia un'infrastruttura tecnologica, cioè *server* virtuali remoti che l'utente finale può utilizzare
- **SaaS** (**Software** as a Service)
  - un fornitore eroga via web una serie di servizi applicativi mettendoli a disposizione degli utenti finali
- **Paas** (**Platform** as a Service)
  - il fornitore offre soluzioni per lo sviluppo e l'*hosting* evoluto di applicazioni. In genere questo tipo di servizi è rivolto a operatori di mercato che li utilizzano per sviluppare e ospitare soluzioni applicative proprie, allo scopo di soddisfare esigenze interne e/o per fornire a loro volta servizi a terzi

Soggetti nello schema Cloud

- **Cliente/Committente** del Cloud Provider/Fornitore
- **Cloud Provider/Fornitore**
- **Sub-contractor** del Cloud Provider/Fornitore

Premessa terminologica

- **Cliente/Committente** del Cloud Provider/Fornitore
  - **Titolare del trattamento / Controller | *Responsabile***
- **Cloud Provider/Fornitore**
  - **Responsabile del trattamento / Processor | *Incaricato***
- **Sub-contractor** del Cloud Provider/Fornitore
  - ***Sub-Incaricato***

Relazione fra Fornitore e Titolare del trattamento

- **La scelta del fornitore** di Cloud rientra nella responsabilità del Titolare del trattamento (**Designazione a Responsabile**)
- Lo squilibrio negoziale (ipotetico) fra il fornitore di Cloud e il Titolare del trattamento **non giustifica** l'accettazione da parte del secondo di clausole o condizioni non conformi alla normativa sulla protezione dei dati

Approccio preliminare

- Analisi dei rischi specifici rispetto al contesto
- Adozione di modelli organizzativi adeguati
- Adozioni di modelli contrattuali / clausole contrattuali specifiche al fine di ottemperare alle responsabilità che comunque incombono sul titolare del trattamento
- Valutazione costo/beneficio «effettiva»
- Esercitare un potere di controllo (*Auditing* e *Logging*)

Rischi specifici

- **Mancanza di controllo**
- **Mancanza di informazioni sul trattamento** che comportano una mancanza di percezione del rischio e delle minacce e dunque la non adozione di appropriate misure

Obiettivi del Titolare del trattamento

- **Disponibilità** dei dati
- **Riservatezza** dei dati
- **Integrità** dei dati
- **Trasparenza** del trattamento
- **Isolamento** dei dati
- **Possibilità di intervento dell'interessato**
- **Responsabilità**
- **Portabilità**

Clausole opportune/necessarie

- **dettagli sulle istruzioni del cliente** (misura e modalità) da trasmettere al fornitore del servizio, con particolare riguardo per gli accordi sul livello del servizio (SLA) applicabili e le sanzioni pertinenti;
- **specificazione delle misure di sicurezza** che il fornitore cloud è tenuto a rispettare, a seconda dei rischi del trattamento e della natura dei dati da proteggere;
- **oggetto e orizzonte temporale** del servizio cloud da fornire, nonché portata, **modalità** e **finalità** del trattamento di dati personali effettuato dal fornitore cloud e **tipologia dei dati** personali oggetto del trattamento;
- specificazione delle **condizioni per la restituzione dei dati** (personali) o per la loro **distruzione** una volta concluso il servizio. Inoltre, occorre garantire la **cancellazione sicura** dei dati personali su richiesta del cliente cloud;
- inserimento di una **clausola di riservatezza** vincolante per il fornitore cloud e per eventuali suoi dipendenti che abbiano accesso ai dati;

Clausole opportune/necessarie

- prevedere l'obbligo a carico del fornitore di **sostenere il cliente nell'agevolare l'esercizio dei diritti degli interessati** di accedere ai loro dati, nonché rettificarli o cancellarli;
- stabilire espressamente che il fornitore cloud **non può comunicare i dati a terzi**, anche per motivi di conservazione, a meno che nel contratto sia prevista la presenza di sub-contraenti;
- chiarire la **responsabilità del fornitore cloud di comunicare** al cliente cloud eventuali **violazioni** che influiscano sui suoi dati;
- obbligo del fornitore cloud di fornire un **elenco dei luoghi** dove può avere luogo il trattamento dei dati;
- diritto del Titolare del trattamento di controllare e corrispondente obbligo del fornitore cloud di cooperare;

Clausole opportune/necessarie

- il contratto dovrebbe stabilire che il fornitore cloud è tenuto a **informare il cliente in merito a cambiamenti rilevanti** concernenti il servizio cloud, come l'attuazione di funzioni aggiuntive;
- il contratto dovrebbe prevedere attività di ***logging*** e ***auditing*** delle operazioni di trattamento di dati personali svolte dal fornitore cloud o da sub-contraenti;
- obbligo generale a carico del fornitore del servizio di assicurare che la sua organizzazione interna e i suoi sistemi di trattamento dei dati (e quelli di eventuali sub-incaricati) sono conformi agli obblighi e alle norme di legge vigenti, nazionali e internazionali.

Categorie tenute al segreto professionale (?!)

- alcuni esempi:
  - Sistemi di archiviazione
    - iCloud (http://www.apple.com/legal/internet-services/icloud/it/terms.html al 20/10/2014)
      - *«tuttavia, Apple si **riserva il diritto in ogni momento di decidere se un Contenuto è opportuno e conforme con il presente Contratto** e può **controllare preventivamente, spostare, rifiutare, modificare e/o rimuovere i Contenuti in ogni momento, senza preavviso e a sua sola discrezione**, nel caso in cui tali Contenuti siano ritenuti in violazione del presente Contratto o siano sgradevoli in altro modo.»*
      - *«rendete atto e accettate che Apple potrà, senza responsabilità nei Vostri confronti, **accedere, utilizzare, conservare e/o divulgare le Vostre informazioni sull'Account e i Contenuti alle forze dell'ordine, funzionari del governo e/o terzi**, così come Apple ritenga sia ragionevolmente necessario o opportuno, qualora sia richiesto per legge o nel caso in cui Apple ritenga in buona fede che tale accesso, uso, divulgazione o conservazione siano ragionevolmente necessari per: (a) conformarsi a procedimenti od ordini giudiziari; (b) applicare il presente Contratto, inclusa l'investigazione di qualsiasi violazione potenziale dello stesso; (c) individuare, prevenire o gestire in altro modo problemi di sicurezza, tecnici o in materia di frode; o (d) proteggere i diritti, la proprietà o la sicurezza di Apple, i suoi utenti, terze parti o il pubblico, così come richiesto o consentito dalla legge.»*
      - *«A eccezione del materiale che noi potremmo concedervi in licenza, Apple non rivendica la proprietà dei materiali e/o dei Contenuti che inviate o rendete disponibili sul Servizio. **Tuttavia, inviando o pubblicando tali Contenuti in aree del Servizio che sono accessibili al pubblico o ad altri utenti per i quali prestate il consenso alla condivisione di tali Contenuti, concedete a Apple una licenza mondiale, gratuita, non esclusiva di utilizzare, distribuire, riprodurre, modificare, adattare, pubblicare, tradurre, rappresentare pubblicamente, e mostrare pubblicamente tali Contenuti** sul Servizio, unicamente ai fini per i quali tali Contenuti sono stati inviati o resi disponibili, senza alcuna retribuzione o obbligazione nei Vostri confronti.»*

Categorie tenute al segreto professionale (?!)

- Google Drive (https://support.google.com/drive/answer/2450387?hl=it al 20/10/2014)
  - «*Quando l'utente carica, trasmette, memorizza, invia o riceve contenuti da o tramite i nostri Servizi,* ***concede a Google (e ai partner con cui collaboriamo) una licenza globale per utilizzare, ospitare, memorizzare, riprodurre, modificare, creare opere derivate (come quelle derivanti da traduzioni, adattamenti o altre modifiche apportate in modo tale che i contenuti funzionino al meglio con i nostri Servizi), comunicare, pubblicare, eseguire pubblicamente, visualizzare pubblicamente e distribuire i suddetti contenuti****. I diritti che concede con questa licenza riguardano lo scopo limitato di utilizzare, promuovere e migliorare i nostri Servizi e di svilupparne di nuovi. Questa licenza permane anche se l'utente smette di utilizzare i nostri Servizi (ad esempio nel caso di una scheda di attività commerciale aggiunta a Google Maps). Alcuni Servizi potrebbero offrire modalità di accesso e rimozione dei contenuti forniti a tale Servizio. Inoltre, in alcuni dei nostri Servizi sono presenti termini o impostazioni che restringono l'ambito del nostro utilizzo dei contenuti inviati a tali Servizi. È necessario assicurarsi di disporre dei diritti necessari per concederci questa licenza rispetto a qualsiasi contenuto inviato ai nostri Servizi.*»

– Servizi di mailing
  - Gmail (https://www.gmail.com/intl/it/mail/help/terms.html al 20/10/2014)
    - «*I nostri sistemi automatizzati* ***analizzano i contenuti dell'utente*** *(incluse le email) al fine di offrire funzionalità dei prodotti rilevanti a livello personale, come risultati di ricerca personalizzati, pubblicità su misura e rilevamento di spam e malware.* ***Questa analisi si verifica nel momento in cui i contenuti vengono trasmessi, ricevuti e memorizzati****.*»

Conclusioni

1) Incentivare l'impiego di **strumenti istituzionali/pubblici**
2) Incrementare la **consapevolezza** negli utenti "professionisti"
3) Ruolo delle Associazioni nella negoziazione delle condizioni di servizio
4) Si configurano **questioni deontologiche** ?

References

1. Parere WP29 05/2012 sul cloud computing
2. Working Paper on Cloud Computing - Privacy and data protection issues, "Sopot Memorandum", 51st meeting, 23-24 April 2012, Sopot (Poland)
3. Relazione del Garante per la protezione dei dati personali, 2013, La protezione dei dati nel cambiamento, Big data, Trasparenza, Sorveglianza
4. Green Paper, Commissione Europea, on mobile Health ("mHealth"), 2014
5. Comunicazione della Commissione Europea, Sfruttare il potenziale del cloud computing in Europa, 2012
6. Mini guida per imprese e pubblica amministrazione del Garante per la protezione dei dati personali, Cloud Computing Proteggere i dati per non cadere dalle nuvole, 2012
7. Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
8. Bozza di regolamento del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)
9. Parere WP29 8/2010 sul diritto applicabile
10. Parere WP29 2/2013 sulle applicazioni per dispositivi intelligenti
11. Decisione della Commissione 5 febbraio 2010, 2010/87/UE, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio
12. ENISA, Good Practice Guide for securely deploying Governmental Clouds
13. ENISA, Survey and analysis of security parameters in cloud SLAs across the European public sector
14. ENISA, Cloud Computing Information Assurance Framework
15. ENISA, Security & Resilience in Governmental Clouds
16. Sopot Memorandum Cloud Computing – Privacy and data protection issues, 23-24 aprile 2012

Michele Martoni

C.I.R.S.F.I.D. | University of Bologna

michele.martoni@unibo.it | (+39) 348.4900232

www.unibo.it | www.cirsfid.unibo.it

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA