Cloud computing ed attività di impresa: la tutela dei dati personali ed aziendali

Firenze, 4 giugno 2011

Alessandro Mantelero

Politecnico di Torino
IV Facoltà

NEXA Center for Internet & Society

http://staff.polito.it/alessandro.mantelero

I. Dal modello proprietario al modello „*as a service*“

modello proprietario:

- fruizione diretta
- controllo diretto

modello *„as a service“*:

- centralità del contratto
- necessità della cooperazione del fornitore del servizio
- contratto di durata: continuità della collaborazione e costante rispetto degli standard (SLA, KPI)
- potenziale rafforzamento delle privative

rischi connessi alla riduzione/perdita di controllo sulle risorse informatiche

criticità:
- dipendenza da controlli indiretti (strumenti software e contrattuali)
- necessità di collaborazione del fornitore (modalità e tempi di intervento)
- lock-in

attività di contrasto:
- rinegoziazione
- soluzioni assicurative per i danni
- selezione degli ambiti da spostare nel cloud
- interoperabilità

II. Dai CED alle *data farm*

rischi „strutturali“
criticità: - maggior appetibilità per i criminali delle grandi concentrazioni di dati
- polverizzazione dei dati ed incertezza sull'effettiva cancellazione
- possibili discontinuità di servizio

attività di contrasto:
- notevoli investimenti in tecnologie difensive ad opera dei fornitori
- esistenza di varie soluzioni tecnico-organizzative
- presenza di norme tecniche

rischi connessi alle dinamiche di mercato
criticità: - processi di concentrazione
- barriere all'interoperabilità
- concentrazione in capo a pochi soggetti di grandi masse di informazioni
- insicurezza geo-politica

attività di contrasto :
- introdurre obbligo di notifica per la creazione dei data center di maggior rilevanza e vigilanza ad opera di organi pubblici ad hoc
- intervento autorità a garanzia della concorrenza
- collaborazione efficiente e rapida a livello globale
- regolamentazione sovranazionale

III. La gestione delle informazioni

ambiti di rilevanza:

- la tutela dei dati personali
- segretezza/riservatezza delle informazioni aziendali (rinvio *supra*)

Il trattamento dati:

- modello „piramidale“

problema di qualificazione:
centralità del rapporto di preposizione e del potere decisionale in capo al preponente, ma non della relazione economico-funzionale fra i soggetti

conseguenze del ruolo ricoperto in termini di:
- obblighi ed oneri di controllo
- adozione e sorveglianza sulle misure di sicurezza
- responsabilità penale, amministrativa e civile

possibili modelli dell'organigramma del trattamento dati nei casi di outsourcing:

I ipotesi: gestione autonoma del trattamento ad opera dell'outsourcee (flusso controller/controller: comunicazione)

vantaggi: parziale trasferimento degli adempimenti, irresponsabilità dell'outsourcer per i danni

svantaggi: mancanza di controllo, obblighi connessi alla comunicazione (informativa e consenso specifico)

II ipotesi: modello in cui l'outsourcer si riserva il controllo della gestione del trattamento effettuato dall'outsourcee (flusso „interno“ controller/processor)

vantaggi: controllo sulla gestione dei dati, superfluità informativa e consenso specifico (natura „interna“ del rapporto)

svantaggi: responsabilità dell'outsourcer per i danni, oneri di controllo e sicurezza

Il rapporto nel cloud computing:

propensione per la qualifica processor (fornitore)/controller (cliente)

indici:

- margine di autonomia decisionale del fornitore
- compiti del fornitore chiaramente e rigorosamente definiti (SLA, KPI, ecc.)
- l'impresa cliente è il soggetto direttamente legittimato dagli interessati a trattare i dati
- il fornitore gestisce le informazioni solamente nell'interesse del cliente
- affidamento al fornitore solamente di parte dei trattamenti
- il fornitore offre servizi di *standard* superiori piuttosto che un elevato grado di autonomia nel trattamento

IV. La gestione dei flussi transfrontalieri di dati

- criterio generale di ammissibilità: flusso verso Paesi terzi solo se viene garantito un livello di protezione adeguato (art. 25, dir. 95/46/CE)

I potesi: adeguatezza del livello di tutela garantito dalla legge del Paese terzo
valutazione positiva della Commissione Europea con riguardo a:
- normativa nazionale del Paese terzo
- accordi ad hoc (caso eccezionale, Safe Harbor)

II ipotesi: inadeguatezza del livello di tutela garantito
- adozione di clausole contrattuali standard definite dalla Commissione (art. 26 § 2, dir. 95/46/CE)
- adozione di clausole contrattuali specifiche ad opera delle parti, con autorizzazione ad hoc dell'autorità nazionale di controllo (art. 26 § 2, dir. 95/46/CE)

III ipotesi: trasferimenti comunque permessi
- consenso dell'interessato, anche implicito (finalità contrattuali o pre-contrattuali)
- dati derivanti da un pubblico registro
- salvaguardia dell'interesse vitale della persona
- salvaguardia di un interesse pubblico rilevante/esercizio diritti in giudizio

II ipotesi: inadeguatezza del livello di tutela garantito (adozione di clausole contrattuali)

a) flusso controller/controller (Paese terzo)
- divieto comunicazione da importatore a ulteriori controller di Paesi terzi (limitate eccezioni)
- responsabilità solidale per i danni agli interessati
- possibilità di agire verso l'esportatore in caso di violazioni dell'importatore

b) flusso controller/processor (Paese terzo)
- disciplina sub-contratto (permane responsabilità primo ricevente)
- vigilanza: autorità di controllo degli stati UE (divieto/sospensione flussi se infrazione)
- legge applicabile al contratto: luogo stabilimento "esportatore"
- azione di danni diretta verso l' "esportatore"
- "clausola del terzo beneficiario" (in contratti fra esportatore,importatore,subincaricato)

c) flusso processor/subprocessor (Paese terzo)
mancanza clausole-tipo fra processor interno/subprocessor di Paese terzo:
- impiego clausole-tipo direttamente ad opera del controller (accordo diretto con il *sub-processor*) o mandato da parte del controller al processor
- accordi contrattuali tra parti (autorizzazione organi di controllo Paese dell'esportatore)