Il Cloud, tra contrattualistica e privacy

aprile2011

PERANI POZZI TAVELLA

Chi Parla?

- Dipartimento di IT di **Perani Pozzi Tavella [2pt.eu]**

- Cultore della materia di Informatica Giuridica, cattedra **Prof. Ziccardi**, Università degli Studi di Milano **[ziccardi.org]**

- Vicepresidente DFA, Digital Forensics Alunmi. **[perfezionisti.it]**

...il resto lo trovate in Rete...

Tra norme e contratti

"*La direttiva europea di protezione dati è del 1995 ed è obsoleta"*(Pizzetti, Cloud Forum 2011).

"*Il contratto ha forza di legge tra le parti"* - art. 1372 c.c.

Il modello Classico

I contratti ad oggetto informatico sono contratti atipici, che possono prevedere obbligazioni di mezzo o di risultato:

- Contratto di licenza Software;
- Contratto di sviluppo Software;
- Contratto di assistenza e manutenzione;
- Contratto di fornitura Hardware;

Il modello Classico

- Molti contratti per differenti oggetti;
- Eventuali contratti collegati;
- Alta negoziabilità;
- Contrattualistica basata sulle richieste del cliente;
- Possibilità di negoziare clausole relative al trattamento dei dati personali.

Il modello Cloud

- Un unico (complesso) contratto per più servizi;
- Bassa negoziabilità del Contratto;
- Difficoltà a negoziare clausole relative al trattamento dei dati.

Dove vanno i dati, chi li tratta...

Con il Cloud non è sempre chiaro chi sono i soggetti che trattano i dati e dove.

Tuttavia, tramite il contratto è possibile delimitare il perimetro.

Dove vanno i dati, chi li tratta...

- divieto esplicito di subappato / subfornitura / subcontratto; (art.1656 c.c.)
- divieto esplicito di cessione;
- indicazione geografica dei server;
- legge applicabile, foro competente (cfr. 2010/87/UE)

Dove vanno i dati, chi li tratta...

Divieto di cessione

“Cloud non può cedere a qualunque titolo il Contratto, in tutto o in parte, ad un altro soggetto, salvo consenso preventivamente prestato in forma scritta da parte di xxx.”

Localizzazione dei Server

“**Cloud** garantisce che i server che verranno utilizzati ai fini dell'adempimento del Contratto sono localizzati presso la sede di Cloud, sita a Milano, in via Bianchi, n.2”

Divieto di subappalto

“Cloud non può subappaltare, in tutto o in parte, le obbligazioni previste dal presente contratto”

Dove vanno i dati, chi li tratta...

Clausola 9 (2010/87/UE)

Legge applicabile

“Le presenti clausole sono soggette alla legge dello Stato membro in cui è stabilito l’esportatore, ossia .....”

Legge e Foro

“Il Contratto è regolato dalla legge italiana. Le Parti pattuiscono che, con riferimento ad ogni e qualsiasi controversia eventualmente scaturente dal Contratto, sarà esclusivamente competente a decidere l’Autorità Giudiziaria del Foro di Milano, impregiudicata la competenza delle Sezioni Specializzate in materia di Proprietà Industriale ed Intellettuale..”

Dove vanno i dati, chi li tratta...

Cosa succede se i dati devono essere esportati all'estero?

Dove vanno i dati, chi li tratta...

- Trasferimento di dati verso isoli 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 Israele, USA (limitatamente alle imprese che aderiscono al c.d. Safe Harbor);
- **Clausole contrattuali** (Cfr. Decisioni della Commissione europea n. 2004/915/CE e 2010/87/UE);
- Binding Corporate Rules (solo all'interno della stessa società);
- Consenso dell'interessato (cfr. art.43 del Codice).

Dove vanno i dati, chi li tratta...

CLAUSOLE CONTRATTUALI TIPO («INCARICATI DEL TRATTAMENTO»)

Ai sensi dell'articolo 26, paragrafo 2, della direttiva 95/46/CE per il trasferimento di dati personali a responsabili del trattamento stabiliti in paesi terzi che non garantiscono un livello adeguato di protezione dei dati

5. Obblighi di Cloud -Cloud, in qualità di importatore dichiara e garantisce quanto segue:

a) di trattare i dati personali esclusivamente per conto e secondo le istruzioni dell'esportatore, nonché a norma delle presenti clausole, e di impegnarsi a informare prontamente l'esportatore qualora non possa per qualsiasi ragione ottemperare a tale disposizione, nel qual caso l'esportatore ha facoltà di sospendere il trasferimento e/o risolvere il contratto;

b) di non avere motivo di ritenere che la normativa ad esso applicabile impedisca di seguire le istruzioni dell'esportatore o di adempiere agli obblighi contrattuali, e di comunicare all'esportatore, non appena ne abbia conoscenza, qualsiasi modificazione di tale normativa che possa pregiudicare le garanzie e gli obblighi previsti dalle presenti clausole, nel qual caso l'esportatore ha facoltà di sospendere il trasferimento e/o di risolvere il contratto;

c) di aver applicato le misure tecniche e organizzative di sicurezza indicate nell'appendice 2 prima di procedere al trattamento dei dati personali trasferiti;(...)

Nomina a Responsabile

Stabilito un “perimetro” è ora necessario stabilire a che titolo vengono trattati i dati dei soggetti terzi, contenuti nelle banche di dati.

Nomina a Responsabile

“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.

Nomina a Responsabile

Gli amministratori di sistema sono *“figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti”* che le *“figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi”*. Detti soggetti svolgono attività quali *"il salvataggio dei dati (backup/recovery), l’organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware”* che *“comportano, infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata, a tutti gli effetti, alla stregua di un trattamento di dati personali; ciò anche quando l'Amministratore non consulti in chiaro le informazioni medesime”*.

Nomina a Responsabile

“La parti concordano che **Cloud**, ai sensi dell’art. 29 del citato Codice della Privacy, sarà Responsabile del trattamento dei dati personali con mansioni di Amministratore di Sistema, conformemente a quanto previsto dal relativo Provvedimento.In ogni caso, i compiti di **Cloud** consistono specificatamente nelle seguenti prestazioni:

a) predisporre sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Tali registrazioni devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

b) (...)

Le parti concordano che, conformemente a quanto previsto dal Provvedimento del Garante xxx potrà procedere ad una verifica - almeno annuale - delle attività svolte da **Cloud**, in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza previste dalle normative vigenti, rispetto ai trattamenti dei dati personali. **Cloud**, inoltre, sarà tenuta, su semplice richiesta di xxx a fornire gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, impiegate presso la propria struttura”.

Sicurezza Informatica

• *“Il diritto, volente o nolente, ha dovuto “mutuare” per certi versi la disciplina informatica della sicurezza, integrandola nei testi di legge”* (Perri, 2003).

• *La Comuntà Europea [...] è impegnata nel promuovere un vero e proprio* ***diritto della sicurezza informatica*** (Cfr. Buttarelli, Verso un diritto della sicurezza informatica in Sicurezza Informatica, 1995)**.**

• *“Nella tematica della sicurezza, l'approccio giuridico non è quello prevalente, ma, nel tempo, la disciplina tecnica si è dovuta coniugare con un insieme di regole simbolicamente contrassegnate come* ***diritto della sicurezza informatica”*** (Buttarelli 1997).

Sicurezza Informatica

• Il diritto della sicurezza informatica ha ad oggetto lo studio delle norme tramite le quali è possibile assicurare **l'integrità**, **la riservatezza** e l**a disponibilità** del **dato** trattato.

Sicurezza Informatica

- Disciplinare l'adozione di misure di sicurezze idonee mediante allegati, prevedendo l'utilizzo di canali crittografati;

- Verifiche sull'adozione (Cfr. 2010/87/UE);

- Risoluzione per inadempimento in caso di mancato rispetto di standard di sicurezza;

- Eventuali penali (Cfr. art. 1382 c.c.).

....continua

Sicurezza Informatica

“Cloud dichiara espressamente di trattare i dati personali di soggetti terzi che le verranno comunicati nell'adempimento del Contratto come previsto dalla attuale normativa in materia di Privacy. **Cloud** dichiara inoltre di adottare misure di sicurezza idonee in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Cloud, in qualsivoglia momento, farà sottoporre gli elaboratori utilizzati per il trattamento dei dati personali, su richiesta dei xxx, a verifiche da parte di quest'ultima e/o da soggetti dalla stessa delegati e/o di un organismo ispettivo composto da soggetti indipendenti, in possesso delle necessarie qualificazioni professionali, vincolati da obbligo di riservatezza e selezionati dall’esportatore, eventualmente di concerto con l’autorità di controllo, al fine di verificare l'effetiva l'adozione delle misure di sicurezza di cui all'articolo precedente”.

Sicurezza Informatica

“Ai sensi e per gli effetti dell’art. 1456 c.c., il Contratto si risolverà di diritto, senza preavviso, in caso di:

a) mancata adozione delle misure di sicurezza di cui all'articolo xx;

b) (..)

In caso di mancata adozione nell'Allegato B, saranno applicate penali a carico di **Cloud** stabilite e quantificate come di seguito:

€ xxx,00 per la mancata adozione di xxxxx;

€ xxx,00 per la mancata adozione di xxxxx;

€ xxx,00 per la mancata adozione di xxxxx;

.E’ comunque fatta salva la risarcibilità di ogni danno ulteriore”.

Sicurezza Informatica

- Esibizione di certificazioni (es. ISO 27001);
- Segnalazione di brecce nella sicurezza e perdite di dati (Security Breach).

Sicurezza Informatica

DIRETTIVA 2009/136/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 25 novembre 2009

recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori

In caso di violazione di dati personali, il fornitore di servizi di comunicazione elettronica accessibili al pubblico comunica senza indebiti ritardi detta violazione all'autorità nazionale competente.

Quando la violazione di dati personali rischia di pregiudicare i dati personali o la vita privata di un abbonato o di altra persona, il fornitore comunica l'avvenuta violazione anche all'abbonato o ad altra persona interessata.

Non è richiesta la notifica di una violazione dei dati personali a un abbonato o a una persona interessata se il fornitore ha dimostrato in modo convincente all'autorità competente di aver utilizzato le opportune misure tecnologiche di protezione e che tali misure erano state applicate ai dati interessati dalla violazione della sicurezza. Tali misure tecnologiche di protezione rendono i dati incomprensibili a chiunque non sia autorizzato ad accedervi.

Sicurezza Informatica

"*Una altra criticità è che la Telecom 2 impone questo obbligo solo ai gestori della banda larga (…) non agli spedizioni dei dati"*(..) "*e questo è un limite"*(Pizzetti, Cloud Forum 2011).

Sicurezza Informatica

“Cloud comunicherà a xxx ogni distruzione o perdita dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme entro 48 ore dal momento della relativa scoperta, mediante una comunicazione a mezzo email da fare pervenire all'indirizzo xxx@xxx.it”.

Clausole Way-Out

- Interoperabilità;
- Distruzione mediante wipeing;
- Restituzione su determinato supporto/formato.

Clausole Way-Out

Non mi sono trovato bene con **Cloud, S.p.A.** voglio passare a **Nuvola S.p.A.**

I dati che mi fornirà **Cloud** possono essere importati su **Nuvola?**

Come assicurare la **disponibilità** del dato?

Clausole Way-Out

“Cloud garantisce sin d’ora che ogni banca di dati contenente dati personali realizzata nell'adempimento del Contratto sarà pienamente compatibile e/o interoperabile con altri componenti Hardware e Software dalla stessa e/o da terzi licenziati e/o forniti e/o con gli Assets di xxx. Ogni banca di dati realizzata nell'adempimento del Contratto sarà basata su **Open Standard**, in modo da offrire il più elevato grado di interoperabilità con altri sistemi. Per Open Standard si intende un linguaggio/formato/protocollo che è:

1. soggetto a una completa valutazione pubblica e a un uso privo di obblighi in modo che sia ugualmente disponibile a chiunque;

2. (...)”.

Clausole Way-Out

"XXX avrà facoltà di richiedere a **Cloud,** in qualsiasi momento, la restituzione della Banca di Dati concesso in licenza a xxx a qualunque titolo e/o con qualsiasi modo messo a disposizione.

xxx avrà altresì la facoltà di richiedere a **Cloud**, in qualsiasi momento, la distruzione integrale o parziale della Banca di Dati e/o ogni altro dato personale consegnato e/o in qualsiasi modo e/o a qualunque titolo messo a disposizione di **Cloud**

La distruzione dei dati dovrà avvenire con modalità atte a cancellarli definitivamente ed irreversibilmente da ogni tipo di supporto, quali, a titolo esemplificativo e non esaustivo, **wiping**, (...)".

GRAZIE

Licenza