diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 10/07/2012

All'indirizzo http://www.diritto.it/docs/33706-cloud-computing-l-opinione-dei-garanti-privacy-europei

Autore: Marcoccio Gloria

Cloud Computing : l’Opinione dei Garanti Privacy Europei

Cloud Computing : l'Opinione dei Garanti Privacy Europei

Gloria Marcoccio (gloria.marcoccio@glory.it)

Giugno 2012

Il primo luglio 2012 il WP 29, consesso dei Garanti Europei per la protezione dei dati personali, ha adottato un'importante opinione riguardo il "Cloud Computing"[1].

Sebbene le opinioni del WP 29 non siano atti con efficacia regolamentare e quindi non comportino di per se nuovi obblighi di legge da rispettare, in ogni caso riflettono la posizione autorevole dei Garanti europei per la protezione dati personali (DPA in seguito) e come tali forniscono importanti indicazioni e precisazioni nella materia affrontata. Se si aggiunge poi che, tipicamente, le Opinioni dei WP 29 emesse su temi importanti (quali ad esempio la videosorveglianza, i sistemi che consentono la geo-localizzazione di individui in tempo reale,…) prima o poi danno luogo a corrispondenti Provvedimenti nazionali dei DPA , questi sì con forza, regolamentare, allora l' Opinione sul Cloud Computing assume, anche in prospettiva, un valore informativo particolare.

Non v'è dubbio che il tema Cloud Computing sia quanto mai popolare ed ampiamente dibattuto per i suoi tanti vantaggi operativi e di riduzioni costi ma anche per i dubbi che si sollevano soprattutto riguardo gli aspetti di sicurezza e di controllabilità dei dati, problematiche contrattuali, conformità alle leggi applicabili.

È un tema complesso, pieno di sfaccettature non certo tutte ancora note ma alla ribalta ormai in tanti contesti, internazionali europei e non[2], nonché nazionali[3]. Quanto poi attiene agli aspetti di protezione dei dati personali e privacy assume una importanza fondamentale, in quanto i dati e i loro trattamenti sono l'oggetto della maggioranza dei servizi interessati al Cloud Computing, che riguardano già adesso ed ancor di più nel futuro pressoché tutti i contesti lavorativi nel settore del privato, nella pubblica amministrazione e nel sociale.

La recente Opinione del WP 29 offre una panoramica delle principali problematiche del Cloud Computing, e fornisce spunti concreti per un approccio sistematico nell'affrontare i rischi derivanti, con indicazioni sulle misure di sicurezza ed accorgimenti nonché tutele sia di natura tecnico/organizzative che di tipo contrattuali, sempre nell'ottica di fornire una guida per operare in modo conforme alle normative privacy europee, essenzialmente le direttive 95/46/EC e 2002/58/EC.

L'Opinione prende in particolar modo in esame il caso, certamente diffuso, in cui il Cliente del servizio Cloud Computing è Titolare del trattamento dati ed il fornitore del servizio è un Responsabile di trattamento dati personali (per l'Italia vedasi come riferimento gli articoli, 4, 28 e 29 del D.Lgs 196/03). Gli Interessati sono coloro i cui dati sono trattati dal Titolare (ad esempio: i dipendenti di un azienda in relazione a servizi di amministrazione interna, i clienti/abbonati dei servizi offerti dall'azienda, i cittadini in relazione a servizi erogati da un ente delle pubblica amministrazione,…).

Le principali fonti di rischi individuate dal WP 29 sono ripartite in termini di:

L'Opinione fornisce un ambito di riferimento per descrivere in modo sistematico i requisiti derivanti dalle normative europee in materia di privacy ed indicare una prima categorizzazione delle contromisure necessarie.

Nella realtà dei fatti, tale ambito dovrà comunque essere contestualizzato nello specifico sistema legislativo applicabile al Cliente: infatti a livello nazionale il recepimento delle direttive europee può comportare particolari adempimenti (esempio per la privacy: verifiche preliminari, autorizzazioni, notifiche al DPA nazionale,…), diversi da paese a paese, il cui rispetto è vincolante per il Cliente (in qualità di Titolare).

Ad esempio in Italia è necessario tenere presenti le misure e gli accorgimenti già individuati dal DPA con i provvedimenti applicabili a servizi erogati in modalità Cloud Computing (a titolo di esempio: il provvedimento sul ruolo dell'amministratore di sistema, il provvedimento sulla sicurezza dei dati di traffico per i servizi di comunicazione elettronica accessibili al pubblico,…).

La prossima figura riassume i principali aspetti del contesto normativo e delle misure individuate dai WP 29.

---

[1] Opinion 05/2012 on Cloud Computing – http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[2] Uno degli ultimi lavori pubblicati dal NIST; Guidelines onSecurity and Privacy in Public Cloud Computing - Special Publication 800-144 - http://www.nist.gov/itl/csd/cloud-012412.cfm;

tutta la attività svolta da ENISA tra cui il recente "ENISA's new guide for monitoring cloud computing contracts" - http://www.enisa.europa.eu/media/press-releases/procure-secure-enisa2019s-new-guide-for-monitoring-cloud-computing-contracts

[3] d'obbligo citare la recente lineguida del DPA italiano: "CLOUD COMPUTING - PROTEGGERE I DATI PER NON CADERE DALLE NUVOLE" - http://www.garanteprivacy.it/garante/doc.jsp?ID=1894503

WP 29 Opinion 5/12: riepilogo dei principali aspetti del contesto normativo e delle misure individuate

Contesto legislativo EU per la protezione dei dati:	
95/46/EC	2002/58/EC

Legge applicabile:

quella del paese(i) ove il Cliente/Titolare è stabilito

Rapporto Cliente-Fornitore-Subfornitori

Essenziale stabilire:
- la ripartizione delle responsabilità per la conformità alla legge
- come consentire in pratica l'esercizio dei diritti degli Interessati

Principi basilari

Trasparenza	Trattamenti limitati alle finalità consentite	Conservazione dati/cancellazione dei dati
• tra Cliente ed Interessati • tra Cliente e Fornitore Chiarezza e completezza nel contratto	Rischi dalla presenza di molti Fornitori/Subfornitori Misure tecniche/organizzative e obbligazioni contrattuali	Necessaria certezza nelle operazioni Misure tecniche/organizzative e obbligazioni contrattuali

Tutele contrattuali, trasferimenti di dati all'estero

- Necessario stabilire un contratto tra Cliente e Fornitore
- Trasferimento di dati verso paesi extra EEA:
  - In generale non applicabili i casi di esenzione previsti dalla 95/46/EC
  - Safe Harbour per i fornitori U.S.A. (comunque per i servizi cloud è opportuno assessment da terza parte)
  - in generale da preferire le clausole contrattuali standard stabilite dalla UE (es. 2010/87/UE) e/o Binding Corporate Rules

Misure tecnico-organizzative:	
Disponibilità dei dati:	Back-up dei dati e procedure di ripristino /Ridondanza di base dati Adeguate caratteristiche del servizio Internet utilizzato
Integrità dei dati:	Intrusion Detection/prevention Systems, Meccanismi di autentificazione crittografica
Riservatezza dei dati:	Dati crittografati sia in "transito" sulla rete sia quando "residenti" sui server Meccanismi di strong authentication per gli utenti (*)
Trasparenza:	Chiarezza e completezza nel contratto
Trattamenti limitati alle finalità consentite	Governance nella distribuzione e nel controllo dei diritti di accesso ai dati personali (*) e Relative misure tecniche
Corrispondere alle richieste di Esercizio dei diritti:	Obbligazioni contrattuali che assicurino al Cliente il supporto del Fornitore (e Subfornitori)
Portabilità dei dati (compatibilità con altri Fornitori-Sistemi)	Verifiche precontrattuali e Obbligazioni contrattuali che assicurino la portabilità al termine del Contratto con il Fornitore (quale ne sia il motivo)
Accountability: *In ambito Information Technology capacità di stabilire cosa è stato fatto e come in un determinato tempo* *In ambito protezione dati la capacità di dimostrare che sono stati prese le appropriate misure ai fini della conformità alla normativa*	Sono richieste misure tecnico-organizzative per dimostrare l'esistenza di una privacy-security Policy e la sua effettiva implementazione, incluse eventuali certificazioni emesse da terze parti. Necessarie apposite obbligazioni contrattuali E' essenziale per consentire al Cliente di corrispondere alle richieste delle autorità competenti (DPA) previste dalla legge *(ad esempio per il caso di "violazione dei dati personali" nei servizi di comunicazione elettronica accessibili al pubblico, introdotto in Italia dal D.Lgs 69/12)*

(*) presso il Fornitore, i Subfornitori, ..ed il Cliente

Il WP 29 pone in particolar modo l'accento sull'esigenza di condurre un' analisi dei rischi, da parte del Cliente, il quale come Titolare rimane direttamente responsabile di fronte la legge in caso di violazioni delle prescrizioni normative applicabili al servizio erogato dal suo Fornitore. Sono evidenti ed espresse dallo stesso WP 29 le criticità nel caso (comunque frequente) in cui i Clienti abbiano un potere contrattuale inferiore a quello del Fornitore: le ripartizioni di responsabilità e l'effettivo controllo loro richiesto in qualità di Titolari appare oggettivamente poco esercitabile nella realtà dei fatti, anche tenendo conto, e ciò rimane valido anche per Clienti medio/grandi, dei costi necessari per eseguire reali e periodici controlli tecnici, operativi e di governance. In tale contesto una strada percorribile, come lo stesso WP 29 rileva, è la attuazione di programmi appositi di certificazioni/audit a cura di terze parti.

Dall'approccio seguito dal WP 29 con questa Opinione ed anche con il suo recente *working document*[4] sulle Binding Corporate Rules applicate nel caso di Fornitore che opera nel ruolo di Responsabile di trattamento dati personali, risulta sempre più evidente che la formazione del rapporto contrattuale tra Cliente e Fornitore di servizio Cloud Computing è snodo essenziale per una impostazione coerente con le effettive necessità del Cliente e gli adempimenti e le responsabilità richieste dalla legge.

Una possibile via da percorrere sembra quella di predisporre le Regole Contrattuali Standard per la formazione di contratti riguardo i servizi erogati in modalità Cloud Computing. Infatti per tali servizi sembrano consolidarsi alcune specifiche peculiarità tra le quali:

- la molteplicità dei Fornitori/Subfornitori coinvolti e la loro dinamicità nel corso della durata del Contratto con il Cliente
- la dislocazione fisica, di principio ovunque nel mondo, dei server utilizzati per i dati e le applicazioni e delle organizzazioni (tecniche che operano su tali dati), le relative esigenze di sincronizzazioni tra i sistemi ai fini della disponibilità ed integrità dei dati,…
- gli aspetti di sicurezza e di continuità di servizio legati sia al Fornitore del servizio di Cloud Computing sia al Internet Service Providers scelti dal Cliente
- il rapporto molto spesso sbilanciato a favore del Fornitore, che spesso non consente di porre in pratica i principi di Trasparenza e soprattutto poi di controllo da parte del Cliente nel suo ruolo di Titolare

….

In un tale contesto le Regole Contrattuali Standard per il Cloud Computing porterebbero ad individuare quelle tipologie di clausole ed allegati che assolutamente non devono mancare in un contratto di servizio erogato in modalità Cloud Computing. Riconoscendo comunque la necessità di stabilire predefiniti criteri di "tailoring" per adattamenti necessari alla reale natura e contesto operativo di uno specifico servizio, tali Regole fornirebbero una base di partenza per operare in accordo al principio di Trasparenza, superare le difficoltà in presenza di sbilanciamento di forza contrattuale tra Cliente e Fornitore, fornire un approccio sistematico e prestabilito per gli aspetti di trasferimenti di dati all'estero (utilizzando in tal caso le apposite decisioni UE) ed operare in concerto con programmi di certificazione / audit in termini di privacy e sicurezza. A tale riguardo è senz'altro da segnalare l' attività di studio in essere presso la Queen University di Londra che ha condotto una serie di survey su diversi contratti Cloud Computing reali, finalizzata ad analizzare il loro livello di adeguatezza[5]. In Italia presso il CSA Italy chapter, capitolo italiano della organizzazione Cloud Security Alliance, a tale proposito è stato attivato uno studio[6] per contribuire alla definizione di Regole standard per la formazione di contratti di servizi Cloud Computing

[4] Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules – http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

[5] **QMUL Cloud Legal Project** - http://www.cloudlegal.ccls.qmul.ac.uk/Research/researchpapers/37188.html

[6] Studio coordinato da G.Marcoccio per CSA Italy Chapter - "Cloud Computing Standard Contractual Clauses": Standard contrattuali come Fattori abilitanti per i servizi cloud – presentato al seminario ISACA 'Cloud Computing' a Roma, 12 giugno 2012