CSA IT Italy Chapter cloud security alliance SM

Cloud Security Alliance Italy Chapter

Studio Data Breach: panoramica degli aspetti normativi ed ottica Cloud

---

Ottobre 2013

Sponsor

TREND MICRO

SafeNet. THE DATA PROTECTION COMPANY

Introduzione

Sistemi informativi e reti di comunicazioni sono entità essenziali per qualunque sviluppo economico e sociale sia in contesti tradizionali sia in ambito *on line* nella *Information & networked society.*

Da sempre le attività di governo per la loro disponibilità & sicurezza richiedono un approccio sistematico e commensurato agli impatti sul business, con processi e soluzioni tecnologiche per:

- rilevare, valutare e comunicare gli incidenti in relazione alla sicurezza delle informazioni
- gestire gli incidenti includendo l'attivazione di misure appropriate per la loro prevenzione (misure ex ante) nonché riduzione e recupero (misure ex post) a fronte degli impatti sul business
- comprendere i punti di debolezza della propria *governance*, valutarli ed affrontarli in modo concreto
- imparare dagli incidenti accaduti e di conseguenza aggiornare il contesto di misure per la gestione della sicurezza delle informazioni

A tali aspetti dettati, in modo diretto, dalla vitale esigenza per le aziende di mantenere ed accrescere il proprio business, si sovrappone sempre più la necessità di conformarsi alla vigente normativa applicabile in tema di violazione dei dati (*data breach*), che in determinati contesti, per la natura ed estensione delle prescrizioni nonché per la severità delle sanzioni previste, assume un importanza tale da divenire essa stessa fattore abilitante per il business.

In ottica Cloud tutto ciò si riflette, ancora una volta, in una particolare attenzione agli aspetti contrattuali ed alle misure di sicurezza, riconfermati come elementi essenziali per il successo di qualunque iniziativa di business basata sul Cloud Computing.

Questo studio propone una panoramica degli aspetti normativi in materia di violazione dati, visti nella più generale ottica di *incident management* sia a livello EU, sia a livello nazionale.

L'attenzione si focalizza in particolare sulla normativa applicabile per i servizi di comunicazione elettronica accessibili al pubblico, per i quali la recente regolamentazione EU ed i conseguenti adeguamenti a livello normativo nazionale delineano un quadro di adempimento assai composito, il cui impianto deve essere adeguatamente calzato nella realtà del business, laddove alla realizzazione ed esercizio di un servizio, concorre una molteplicità di fornitori e subfornitori. Certamente un contesto da tenere presente per i servizi basati sul Cloud Computing.

.

Indice

Si ringrazia

Coordinatore del Gruppo di Lavoro

Valerio Vertua

Autori/Contributori

Gloria Marcoccio (Team Leader)

Ingegnere, senior consultant tecnico/legale per le implementazioni derivanti da standard e normative nazionali ed internazionali nel contesto ICT, nuove tecnologie e sicurezza. Esperto indipendente e revisore di progetti EU, autrice di articoli, libri e saggi.

Nicola Fabiano

Avvocato Cassazionista, Specialista in Diritto Civile, Privacy by Design Ambassador, Consulente a progetti europei, esperto legale per security, ICT e nuove tecnologie, autore di articoli, libri e saggi.

Simone Colangeli

Avvocato del Foro di Roma, fiduciario di primario Gruppo Bancario, difensore di fiducia di personale diplomatico, consulente legale nel settore delle nuove tecnologie e per le problematiche di sicurezza

Riccardo Canetta

Con un background nelle telecomunicazioni, da più di 5 anni lavora come sales manager nel settore della sicurezza IT: in SafeNet segue importanti clienti nei settori Finance, Difesa, PA e Telco, affrontando quindi quotidianamente tematiche come la protezione dei dati, la compliance e la sicurezza delle informazioni, anche in cloud.

Review

Comitato Direttivo CSA Italy

Comitato Scientifico CSA Italy

Sponsor

SafeNet

Trend Micro

1.0 Argomenti trattati

Lo studio riguarda la normativa a livello EU e nazionale per quanto concerne la violazione dei dati con particolare riferimento alla violazione dei dati personali nei servizi di comunicazione elettronica accessibili al pubblico, in quanto in tale settore in Italia è vigente una apposita normativa, di considerevole impatto sotto molteplici profili. Lo studio include diversi schemi di sintesi allo scopo di evidenziare i requisiti normativi con particolare riguardo agli aspetti implementativi che ne conseguono ed un approfondimento riguardo le misure di sicurezza, in supporto agli adempimenti previsti da tale normativa. Relativamente agli aspetti contrattuali tra le parti coinvolte nell'erogazione di un servizio oggetto della normativa sulla violazione dei dati personali, in appendice 1 è riportata una traccia con lo scopo di evidenziare alcuni degli aspetti che meritano attenzione. In appendice 2 sono sinteticamente riportati i risultati della survey avviata quest'anno da CSA ITALY CHAPTER come parte integrante di questo studio.

Nota - tutti gli hyperlink riportati nel testo si intendono e sono stati utilizzati così come resi disponibili dalle relative organizzazioni responsabili, con validità visionata al: 30 Giugno 2013.

2.0 Contesto normativo a livello EU

Come evidente dall'attuale evoluzione del nostro sistema legislativo, gran parte delle normative dei paesi appartenenti alla Unione Europea è di origine comunitaria sia in modo diretto (ad esempio: tramite i Regolamenti) sia come trasposizione nell'ordinamento legislativo nazionale del singolo paese Membro (come nel caso delle Direttive). Occorre poi aggiungere che anche per molti paesi, non Membri EU, la normativa comunitaria di alcuni settori è comunque vincolante (è il caso dei paesi aderenti allo spazio economico europeo- EEA) o tale da essere considerata come un importante esempio, di indirizzo per sviluppare le proprie normative nazionali (è il caso di alcuni dei paesi dell'America Latina).

Pertanto il contesto normativo europeo e gli organismi di riferimento che svolgono direttamente o meno un ruolo nell'applicazione delle normative comunitarie hanno nel loro insieme un'innegabile importanza anche in ambito normativa sulla violazione dei dati, che deve essere tenuta ben presente dagli operatori di servizi basati sul Cloud Computing .

2.1 Principali organismi di riferimento

La normativa comunitaria è prodotta dal **Parlamento Europeo** e dal **Consiglio Europeo** tipicamente su proposta della **Commissione Europea.**

Quest'ultima in particolare ha due Commissioni di essenziale rilevanza per i temi di questo studio:

Justice Fundamental Rights and Citizenship presieduta da Viviane Reding

e

Digital Agendafor Europe (DAE) presieduta da Neelie Kroes

In relazione al tema qui di interesse, la **Justice Fundamental Rights and Citizenship** ha proposto all'inizio del 2012 una profonda revisione delle normative europee in materia di protezione dati personali e privacy, includendo specifiche prescrizioni anche in tema di violazione dei dati personali (vedasi prossimi paragrafi).

Il programma di attività attuale della **Digital Agenda** è suddivisa per Pilastri (Pillars)

Pillar I: Digital Single Market
Pillar II: Interoperability & Standards
Pillar III: Trust & Security
Pillar IV: Fast and ultra-fast Internet access
Pillar V: Research and innovation
Pillar VI: Enhancing digital literacy, skills and inclusion
Pillar VII: ICT-enabled benefits for EU society

dei quali il terzo (Trust & Security) include specifiche azioni per la cyber security, tra cui l'istituzione di appositi organismi di controllo (come è il caso del European Cybercrime Centre- EC3), il potenziamento di agenzie europee già esistenti (parliamo di ENISA) in un contesto di strategie contro il *cyber crime* che prevedono anche la proposta di una apposita nuova direttiva (NIS Directive, vedasi prossimi paragrafi), il tutto con profonde correlazioni con quanto attiene la gestione degli incidenti e le violazioni dei dati.

L'**European Cybercrime Centre- EC3**[1], ospitato presso l'Europol[2], attivo a partire dal Gennaio 2013, istituito con apposita azione della Digital Agenda, ha il compito di agire come *focalpoint* nella lotta EU contro il *cyber crime* contribuendo a velocizzare le reazioni in caso di crimini commessi *on line* e inoltre deve supportare gli Stati Membri e le istituzioni dell'Unione Europea nel realizzare capacità operative e di analisi per attività investigative e cooperazioni internazionali.

[1] https://www.europol.europa.eu/ec3

[2] http://www.europol.europa.eu/

ENISA[3] è invece l'agenzia europea con il ruolo di centro di competenza EU per la sicurezza delle reti e dell'informazione, istituita a partire dal 2004 per migliorare la capacità della Unione Europea, degli Stati Membri e la comunità del business nel prevenire, indirizzare e rispondere a problematiche inerenti appunto la sicurezza delle reti e delle informazioni. Sullo scenario internazionale ENISA può essere paragonata, sul piano degli intenti, al centro di competenza statunitense NIST[4].

Occorre poi menzionare il **Working Party 29**[5], consesso dei garanti privacy[6] dei paesi Membri EU, istituito tramite appunto l'articolo 29 della vigente direttiva europea 95/46/EC in materia di protezione dati personali e privacy, che ha il compito di assistere le istituzioni europee in tale materia. Sebbene non sia un organismo dotato di poteri decisionali, ha comunque una grande influenza sulla impostazione della normativa in questione e di conseguenza sui provvedimenti emanati a livello di singolo stato Membro proprio perché il WP 29 è formato dalle autorità nazionali competenti per la privacy e protezione dati personali.

Infine occorre citare l'**European Data Protection Supervisor (EDPS)**[7] autorità indipendente Europea il cui principale obiettivo è assicurare che le istituzioni e gli enti Europei rispettino il diritto alla privacy e alla protezione dei dati personali nel trattamento dei dati per loro finalità e scopi e nello sviluppo di nuove politiche. L'EDPS opera in base alla apposita Regulation 45/2001, ed è presieduto attualmente da Peter Hustinix (coadiuvato da Giovanni Buttarelli nel ruolo di Assistant Supervisor).

Sul versante degli standard internazionali e dunque di quelle normative che, pur non avendo la forza di un obbligo di legge, di fatto stabiliscono requisiti essenziali e di riferimento per il business, occorre senz'altro tenere presente l'ente **ISO** (International Organization for Standardization)[8].

Qui di seguito uno schema di sintesi dei principali organismi fin qui menzionati.

[3] http://www.enisa.europa.eu/

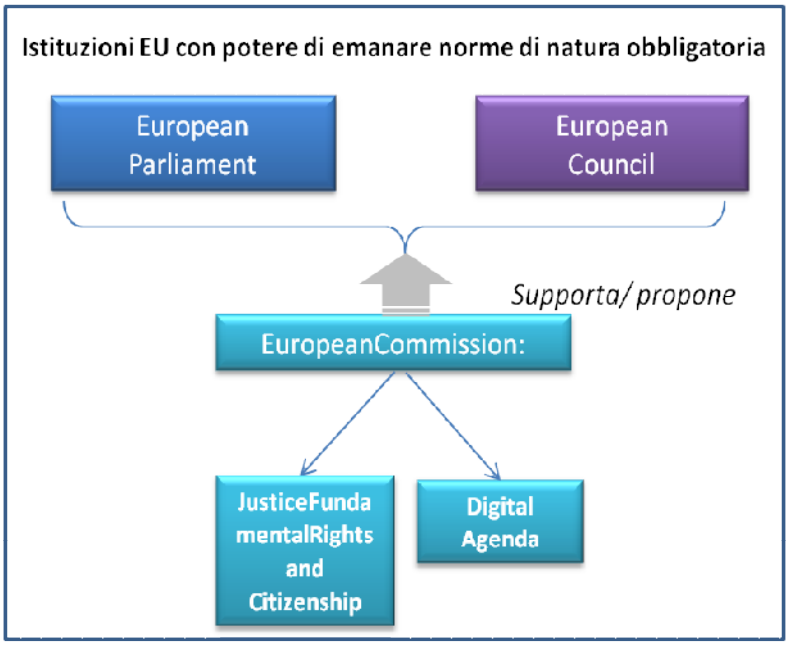
[4] http://www.nist.gov/index.html

[5] http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

[6] Dizione correntemente utilizzata per denotare in breve le autorità garanti per la protezione dei dati personali, istituite con la direttiva europea 95/46/CE

[7] http://www.edps.europa.eu/EDPSWEB/

[8] http://www.iso.org/iso/home.html



2.2 Normativa vigente

Per normativa in materia di violazione dei dati qui si intende in generale quel complesso di prescrizioni che richiedono l'adozione di:

I. Misure di sicurezza preventive tali da minimizzare 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 loro raccolta
II. Misure in grado di individuare l'insorgenza di una violazione dei dati
III. Misure di sicurezza da attivare ex post in caso di insorgenza di una violazione dei dati allo scopo di limitarne i danni
IV. Misure per la notificazione agli utenti coinvolti dalla violazione e/o alle autorità competenti
V. Misure per la gestione dell'incidente di violazione dei dati

Vi è poi da tenere presente la natura dei dati, che per le finalità di questo studio possiamo classificare in termini di:

1. Dati personali
2. Altri dati, non personali

Ulteriormente risulta opportuno schematizzare anche i settori di business in termini di:

A. servizi della società dell'informazione[9]
B. servizi di comunicazioni elettroniche accessibili al pubblico[10]
C. altri settori di business non necessariamente svolto *on line*

Queste tre tipologie di precisazioni costituiscono una sorta di sistema di riferimento, che ci consente di schematizzare in che modo, parzialmente o in toto, risulta applicabile la attuale normativa EU di interesse, e quella proposta, per la quale è stato già avviato il processo di analisi per la successiva promulgazione a livello EU.

[9]Come definiti con la direttiva europea in materia di commercio elettronico 2000/31/CE
[10]Come definiti con la direttiva europea in materia di comunicazioni elettroniche 2002/58/CE

La seguente tabella referenzia schematicamente le vigenti normative EU di interesse, in termini di loro copertura ed applicabilità rispetto al sistema di riferimento sopra definito.

Sistema di riferimento	Direttiva 95/46/CE per la tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali	Direttiva 2002/58/CE, direttiva relativa alla vita privata e alle comunicazioni elettroniche come modificata dalla Direttiva 2009/136/CE	Direttiva 2008/114/CE relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione
1. Dati personali	X	X	
2. Altri dati, non personali			X
A. servizi della società dell'informazione	X		
B. servizi di comunicazioni elettroniche accessibili al pubblico	X	X	
C. altri settori per business non necessariamente svolto on line	X		X
I. Misure di sicurezza preventive tali da minimizzare ii 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 loro raccolta	X ART. 17	X ART. 4	X ART. 5 e Allegato II (MA NON ESPLICITAMENTE)
II. Misure in grado di individuare l'insorgenza di una violazione dei dati		X ART. 4	X ART. 5 e Allegato II (MA NON ESPLICITAMENTE)
III. Misure di sicurezza da attivare ex post in caso di insorgenza di una violazione dei dati allo scopo di limitarne i danni		X ART. 4	X ART. 5 e Allegato II (MA NON ESPLICITAMENTE)
IV. Misure per la notificazione agli utenti coinvolti dalla violazione e/o alle autorità competenti		X ART. 4	
V. Misure per la gestione dell'incidente di violazione dei dati		X ART. 4	X ART. 5 e Allegato II (MA NON ESPLICITAMENTE)

Pertanto, come si deduce dallo schema precedente,attualmente è in vigore a livello EU una esplicita e completa normativa solo per il caso di violazione di dati personali nel contesto dei servizi di comunicazioni elettroniche accessibili al pubblico.

A partire dal 25 Agosto entrerà poi in vigore in tutti i paesi Membri UE il Regolamento n.611/2013[11] in materia di comunicazione delle violazioni di dati personali, nel settore dei servizi di comunicazioni elettroniche accessibili al pubblico. In quanto Regolamento, questa normativa sarà direttamente in vigore senza necessità di essere trasposta nei singoli ordinamenti legislativi nazionali.

Sistema di riferimento	**Regolamento EU 611/2013**
1. Dati personali	X
2. Altri dati, non personali	
A. servizi della società dell'informazione	
B. servizi di comunicazioni elettroniche accessibili al pubblico	X
C. altri settori per business non necessariamente svolto on line	
I. Misure di sicurezza preventive tali da minimizzare ii 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 loro raccolta	X ART. 4 (ININTELLIGIBILITÀ DEI DATI)
II. Misure in grado di individuare l'insorgenza di una violazione dei dati	X ART. 2 para. 3
III. Misure di sicurezza da attivare ex post in caso di insorgenza di una violazione dei dati allo scopo di limitarne i danni	
IV. Misure per la notificazione agli utenti coinvolti dalla violazione e/o alle autorità competenti	X ART. 2 ART. 3 ART. 5
V. Misure per la gestione dell'incidente di violazione dei dati	

Di seguito riportiamo un breve commento rispetto le disposizioni presenti nelle 3 direttive e nel recente regolamento relativamente agli aspetti di violazione dei dati.

[11]REGOLAMENTO (UE) N. 611/2013 DELLA COMMISSIONE del 24 giugno 2013 sulle misure applicabili alla notifica delle violazioni di dati personali a norma della direttiva 2002/58/CE del Parlamento europeo e del Consiglio relativa alla vita privata e alle comunicazioni elettroniche

2.2.1 Direttiva 96/46/CE

La direttiva 95/46/CE, specifica per il trattamento dei dati personali e valida in pressoché tutti i settori di business ove avviene trattamento di tali dati, con il suo art. 17 richiede l'adozione di adeguate misure per contenere i rischi ai quali possono essere soggetti i dati e quindi contiene già un obbligo diciamo di carattere generale a limitare la possibilità di insorgenza di violazione dei dati personali. Nulla invece di obbligatorio in termini di trattazione di una violazione, misure ex post né tantomeno obblighi di notificazioni ad autorità competenti o ai diretti interessati e relative tempistiche.

2.2.2 Direttiva 2002/58/CE come modificata dalla direttiva 2009/136/CE

La direttiva 2002/58/CE come modificata dalla direttiva 2009/136/CE[12] presenta invece tutti gli specifici obblighi per la violazione di dati personali, obbligatori nel settore dei servizi di comunicazioni elettroniche accessibili al pubblico. Ricordiamo che a livello EU il quadro normativo vigente in tale settore è rappresentato dal seguente framework di direttive.

La direttiva 2009/136/CE è l'esplicita fonte degli obblighi in materia di violazione di dati personali in vigore attualmente nella UE e di conseguenza in Italia, tramite le modifiche apportate al Codice Privacy (D.Lgs 196/03) dal decreto legislativo di recepimento della direttiva stessa (D.Lgs 69/12), presentate nel successivo capitolo.

[12]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

Nell'art. 2 della direttiva è riportata la definizione di "violazione dei dati personali"

> *violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico*

Nella definizione è importante notare che la violazione presuppone l'esistenza di misure di sicurezza che vengono appunto violate (*violazione della sicurezza…)*. In estrema sintesi con l'articolo 4 della direttiva è richiesto al fornitore di servizi di comunicazione elettronica accessibili al pubblico di provvedere per:

- dati personali accessibili soltanto al personale autorizzato per fini legalmente autorizzati
- dati personali archiviati o trasmessi dalla distruzione accidentale o illecita, da perdita o alterazione accidentale e da archiviazione, trattamento, accesso o divulgazione non autorizzati o illeciti, e
- attuazione di una politica di sicurezza in ordine al trattamento dei dati personali
- in caso di avvenuta violazione di dati personali:
    - comunicazione 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: comunicazione dell'avvenuta violazione anche all'abbonato o ad altra persona interessata; non è richiesta tale comunicazione se il fornitore ha dimostrato 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 devono essere tali da rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi.
    - la comunicazione all'abbonato o ad altra persona: contiene almeno una descrizione della natura della violazione di dati personali e i punti di contatto presso cui si possono ottenere maggiori informazioni ed elenca le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione di dati personali.
    - la comunicazione all'autorità nazionale competente: descrive, inoltre, le conseguenze della violazione di dati personali e le misure proposte o adottate dal fornitore per porvi rimedio.
- mantenere un inventario delle violazioni dei dati personali, ivi incluse le note riguardi le circostanze in cui si sono verificate, le loro conseguenze e i provvedimenti adottati per porvi rimedio, in misura sufficiente per consentire alle autorità nazionali competenti le verifiche di loro responsabilità

2.2.3 Direttiva 2008/114/CE

Per le infrastrutture critiche esiste apposita direttiva 2008/114/CE[13], 8 Dicembre 2008, esplicitamente indirizzata ai settori dell'**Energia e dei Trasporti.**

Per Infrastruttura Critica la direttiva intende:

> *un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni;*
>
> *"infrastruttura critica europea" è un'infrastruttura critica ubicata negli Stati membri il cui danneggiamento o la cui distruzione avrebbe un significativo impatto* ***su almeno due Stati membri****. …*

In Italia il recepimento della direttiva 2008/114/EC è avvenuto con il Decreto Legislativo 61/2011 (vedasi successivo capitolo).

La direttiva richiede agli stati Membri di adottare misure allo scopo di individuare, secondo un determinato criterio, quali infrastrutture debbano essere trattate come critiche, definire punti di contatto che consentano un coordinamento a livello UE per quanto attiene la sicurezza di tali infrastrutture e richiede che sia adottato, per ogni infrastruttura critica, un Procedura per il Piano di Sicurezza degli Operatori PSO (Operator Security Plan). Il PSO deve includere anche l'individuazione, la selezione e la previsione di priorità per contromisure e procedure, con una distinzione fra:

- misure permanenti di sicurezza, che individuano gli investimenti e gli strumenti indispensabili in materia di sicurezza che si prestano ad essere utilizzati in ogni momento. Rientrano sotto questa voce le informazioni riguardanti le misure di tipo generale, quali quelle tecniche (inclusa l'installazione di strumenti di rilevazione,
  controllo accessi, protezione e prevenzione); le misure organizzative (comprese le procedure di allarme e gestione delle crisi); le misure di controllo e verifica; le comunicazioni; la crescita della consapevolezza e l'addestramento; la sicurezza dei sistemi informativi,

- misure graduali di sicurezza, che possano essere attivate in funzione dei diversi livelli di rischio e di minaccia.
  Fra queste misure sono quindi da considerarsi sottese quelle per la gestione degli incidenti e relativa comunicazione ai punti di contatto nel singolo Stato Membro, che includono necessariamente quanto attiene anche agli incidenti che riguardano i dati trattati per l'operatività e gestione delle infrastrutture critiche.

[13] DIRETTIVA 2008/114/CE DEL CONSIGLIO dell'8 dicembre 2008 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione

2.2.4 Il regolamento EU 611/2013

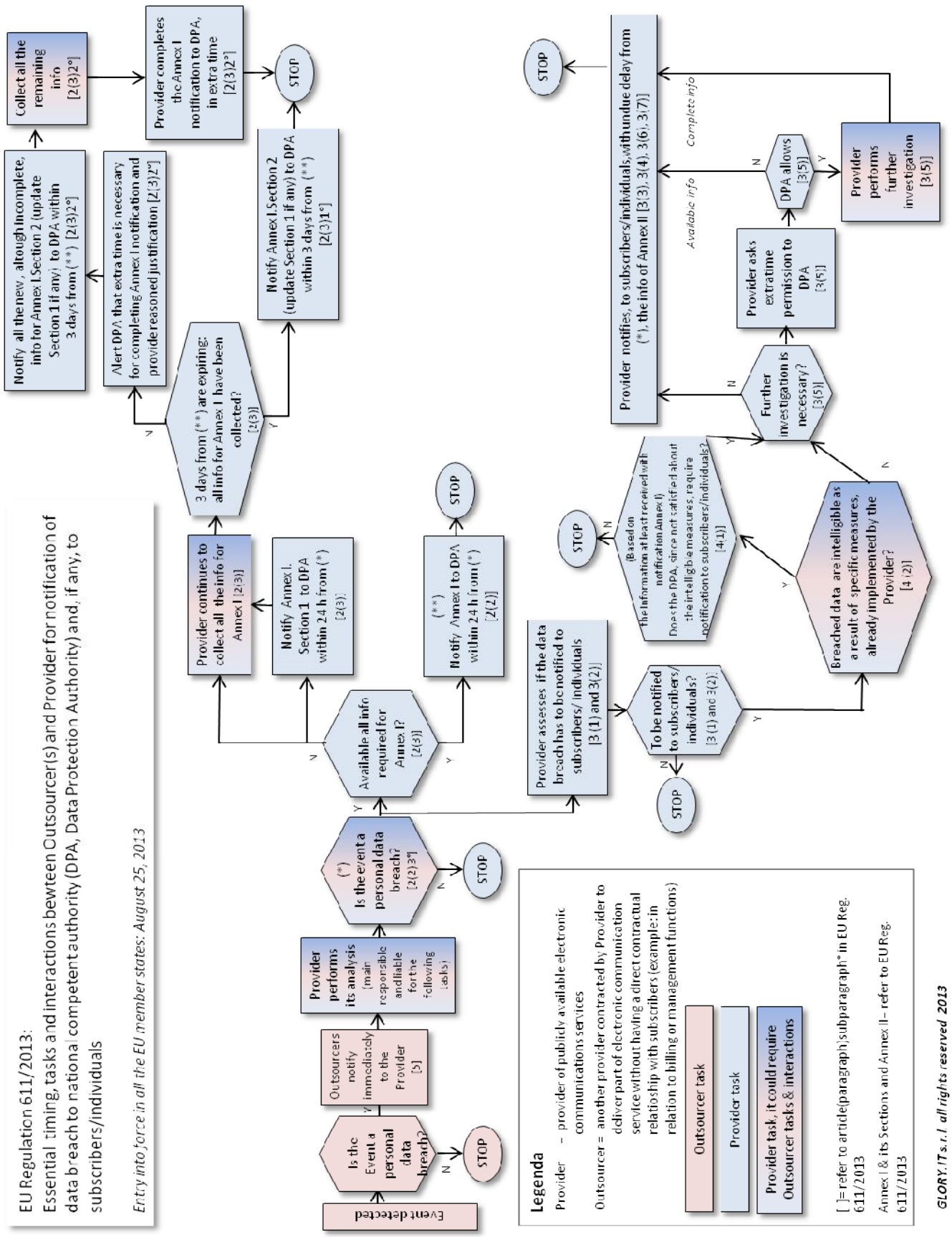
La Commissione Europea con il Regolamento pubblicato sulla Gazzetta Ufficiale Europea il 26 giugno 2013, in vigore in tutti i paesi membri UE a partire dal 25 agosto 2013 introduce nuove regole su come esattamente gli operatori delle telecomunicazioni e i fornitori di servizi Internet (ISP) debbano comportarsi in caso di perdita, furto o compromissione in altro modo dei dati personali dei loro clienti, con il fine ultimo di garantire che, in caso di violazione di dati, tutti i clienti ricevano un trattamento equivalente in tutta l'Unione europea e le imprese possano adottare un approccio paneuropeo a tale problema nel caso in cui operino in più di un paese.

Da un punto di vista operativo, laddove in ambito nazionale sono già state predisposte specificazioni analoghe come è appunto il caso dell'Italia con l'apposito Provvedimento del 4 aprile 2013 del Garante privacy italiano, le aziende destinatarie dei requisiti sono chiamate ad operare con la dovuta attenzione, qualora rimangono aspetti non omogenei tra le due diverse fonti normative per non incorrere nelle severe sanzioni previste nel contesto nazionale.

Da notare che il garante privacy italiano si è riservato di rivedere il proprio provvedimento del 4 aprile qualora emergano differenti orientamenti in termini di tempi e contenuti delle comunicazioni da inoltrare appunto in caso di violazioni dei dati personali.

Dalla lettura del Regolamento risultano effettive differenze: occorrerà comunque vedere quale sarà, nei tempi e nei modi, l'intervento di armonizzazione a cura del Garante privacy italiano.

Al fine di fornire una veduta di assieme degli adempimenti richiesti esplicitamente alle aziende destinatarie della regolamentazione in oggetto, qui di seguito è riportato un unico quadro per descrivere sinteticamente le tempistiche, i compiti e le interazioni conseguenti per esse.


EU Regulation 611/2013:
Essential timing, tasks and interactions bewteen Outsourcer(s) and Provider for notification of data breach to national competent authority (DPA, Data Protection Authority) and, if any, to subscribers/individuals
Entry into force in all the EU member states: August 25, 2013
Event detected
Is the Event a personal data breach?
STOP
Outsourcers notify immediately to the Provider [3]
Provider performs its analysis (main responsible and liable for the following tasks):
(*) Is the event a personal data breach? [2(2)3°]
STOP
Available all info required for Annex I? [2(3)]
Provider continues to collect all the info for Annex I [2(3)]
Notify Annex I, Section 1 to DPA within 24 h from (*) [2(3)]
3 days from (**) are expiring: all info for Annex I have been collected? [2(3)]
Notify all the new, altough incomplete, info for Annex I, Section 2 (update Section 1 if any) to DPA within 3 days from (**) [2(3)2°]
Alert DPA that extra time is necessary for completing Annex I notification and provide reasoned justification [2(3)2°]
Collect all the remaining info [2(3)2°]
Provider completes the Annex I notification to DPA, in extra time [2(3)2°]
STOP
Notify Annex I, Section 2 (update Section 1 if any) to DPA within 3 days from (**) [2(3)1°]
STOP
(**) Notify Annex I to DPA within 24 h from (*) [2(2)]
STOP
Provider assesses if the data breach has to be notified to subscribers/ individuals [3(1) and 3(2)]
To be notified to subscribers/ individuals? [3(1) and 3(2)]
STOP
(Based on the information at least received with notification Annex I) Does the DPA, since not satisfied about the intelligibe measures, require notification to subscribers/individuals? [4(1)]
STOP
Breached data are intelligible as a result of specific measures, already implemented by the Provider? [4(2)]
Further investigation is necessary? [3(5)]
Provider asks extratime permission to DPA [3(5)]
DPA allows [3(5)]
Provider performs further investigation [3(5)]
Provider notifies, to subscribers/individuals, with undue delay from (*), the info of Annex II [3(3), 3(4), 3(6), 3(7)]
Available info
Complete info
STOP
Legenda
Provider – provider of publicly available electronic communications services
Outsourcer = another provider contracted by Provider to deliver part of electronic communication service without having a direct contractual relationship with subscribers (example: in relation to billing or management functions)
Outsourcer task
Provider task
Provider task, it could require Outsourcer tasks & interactions
[ ]= refer to article(paragraph),subparagraph° in EU Reg. 611/2013
Annex I & its Sections and Annex II – refer to EU Reg. 611/2013
GLORY.ITs.r.l. all rights reserved 2013

2.3 Linee Guida/standard

Con riferimento agli enti EU/internazionali menzionati all'inizio del capitolo, qui di seguito si riporta un breve riepilogo dei loro principali lavori e standard attinenti alla gestione degli incidenti che riguardano le informazioni, tra i quali è ricompreso il caso di violazione dei dati personali.

2.3.1 ENISA

Data breach notifications in the EU - Jan 13, 2011

Il sistema europeo di notifica delle violazione di dati nel settore delle comunicazioni elettroniche, introdotto con la revisione della direttiva e-privacy (2002/58/CE) a seguito della direttiva 2009/136/EC, è considerato un importante passaggio per aumentare il livello di sicurezza dei dati in Europa e rassicurare i cittadini sulla protezione dei loro dati personali a cura degli operatori del settore della comunicazione elettronica. In questo contesto, ENISA ha esaminato la situazione al fine di sviluppare un insieme coerente di linee guida relative alle misure tecniche di attuazione e procedure relative, come descritto all'articolo 4 della direttiva 2002/58/CE

Good Practice Guide for Incident Management, 2010

Questa guida integra il set di guide predisposto da ENISA per supportare i CSIRT - Computer Emergency Response Teams.

ENISA Threat Landscape, 8 Gennaio 2013

Questo report fornisce una panoramica aggiornata di minacce e relativi trend, realizzato sulla base di moltissimi contributi da parte di istituti scientifici, enti di standardizzazioni, aziende leader nel settore della sicurezza delle informazioni.

Critical Cloud Computing - A CIIP perspective on cloud computing services- Version 1,0, Dicembre 2012

Questo report analizza il contest del cloud computing dal punto di vista CIIP (Critical Information Infrastructure Protection) considerando diversi scenari e minacce, sulla base di informazioni pubbliche in merito all'adozione del cloud computing e relativi attacchi informatici di grandi dimensioni nonché interruzioni di tali servizi.

2.3.2 NIST

SP 800 61 Rev 2 Computer Security Incident Handling Guide, August 2012

Questa guida, di grande rilievo come impostazione e sistematicità nel trattare i temi in oggetto, fornisce un supporto di base alle organizzazioni che intendono stabilire una struttura per gestire *computer security incident*.

2.3.3 ISO

ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management

Questo standard fornisce una guida sistematica per la gestione di incidenti in relazione alla sicurezza delle informazioni ed è rivolto ad aziende di medio grandi dimensioni. Le organizzazioni più piccole[14] possono usare un set base dei documenti, processi e procedure descritte nello standard in funzione delle loro dimensioni e del loro business in relazione alle situazioni di effettivo rischio.

2.3.4 Cloud Security Alliance

Occorre poi ricordare che Cloud Security Alliance nell'ambito delle sue attività per promuovere l'uso di best practicesin relazione alla sicurezza nei servizi Cloud Computing, ha prodotto una guida apposita nella quale (capitolo 9)sono trattati anche gli aspetti relativi all'incident management.

Security Guidance for Critical Areas of Focus in Cloud Computing V3.0

[14] *definizione EU per micro impresa, piccola e media impresa:http://europa.eu/legislation_summaries/other/n26001_it.htm*

2.4 Proposte normative EU in materia di violazione dati

La seguente tabella referenzia schematicamente le nuove normative proposte a livello EU di interesse per la violazione dei dati sempre in termini di loro futura copertura ed applicabilità rispetto al sistema di riferimento definito all'inizio di questo capitolo.

Sistema di riferimento	**La proposta di nuova regolamentazione privacy** ***Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*** Stato dei lavori presso il Parlamento Europeo Documento originale come presentato dalla Commissione Europea il 25.1.2012	**La proposta di direttiva NIS** ***Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union*** Documento originale come presentato dalla Commissione Europea l'8.2.2013
1. Dati personali	X	X
2. Altri dati, non personali		X
A. servizi della società dell'informazione	X	X
B. servizi di comunicazioni elettroniche accessibili al pubblico	X	
C. altri settori per business non necessariamente svolto on line	X	X
I. Misure di sicurezza preventive tali da minimizzare ii 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 loro raccolta	X ART. 30	X ART.14
II. Misure in grado di individuare l'insorgenza di una violazione dei dati	X ART. 31 (IMPLICITO)	X ART.14 (IMPLICITO)
III. Misure di sicurezza da attivare ex post in caso di insorgenza di una violazione dei dati allo scopo di limitarne i danni	X ART.31	X ART.14 (IMPLICITO)
IV. Misure per la notificazione agli utenti coinvolti dalla violazione e/o alle autorità competenti	X ART.. 31 E ART. 32	
V. Misure per la gestione dell'incidente di violazione dei dati	X ART.31	X ART.14 (IMPLICITO)

2.4.1 Proposta di nuova privacy regulation EU

La proposta di nuova legislazione EU in materia di privacy & protezione dei dati personali in luogo della attuale direttiva 95/46/CE è stata presentata dalla Commissione Europea il 25 gennaio 2012 ed è in corso il

processo, non senza difficoltà, per la sua promulgazione, tenendo anche presente che si tratta di regolamentazione e non di direttiva, pertanto si applicherà direttamente senza processo di trasposizione da parte degli Stati Membri EU.

La proposta include specifici requisiti di violazione di dati personali, sulla falsariga di quelli già presenti nella direttiva in vigore 2002/58/EC indirizzata ai fornitori di servizi di comunicazione elettronica accessibili al pubblico (vedasi precedenti paragrafi). In aggiunta rispetto alla formulazione dei requisiti nella direttiva 2002/58/EC occorre notare che in relazione a tali obblighi è esplicitamente menzionato anche il Processor ossia il provider di servizi che comportano trattamento di dati personali per finalità e scopi del Controller (titolare dei trattamenti),quest'ultimo naturale destinatario delle prescrizioni della proposta Regulation. L'attuale normativa italiana in materia di violazione dei dati personali,ricordiamo: esclusivamente per il settore dei servizi di comunicazione elettronica accessibili al pubblico, ha in pratica già prescritto in merito a questo coinvolgimento diretto del Processor in relazione agli obblighi in materia di violazione dei dati personali, come sarà descritto nel capitolo dedicato appunto alla normativa italiana.

La proposta attuale presenta diversi aspetti critici da molteplici punti di vista, tra i quali:

- in primo luogo la natura stessa dell'atto in quanto trattasi di Regolamento e non di Direttiva, come tale direttamente applicabile in tutti i Paesi Membri UE senza necessità di trasposizione nei singoli ordinamenti legislativi nazionali, come è invece il caso della Direttiva
- la ripartizione di competenze e poteri di intervento che tendono ad essere accentrati sulla Commissione Europea a discapito dell'attuale schema basato pienamente sulle autorità nazionali competenti in materia di privacy e protezione dati personali
- l'applicabilità della norma europea anche a fornitori di servizi stabiliti al di fuori dell'Unione, quando i loro servizi vengono offerto all'interno delle UE
- un apparato di adempimenti assai complesso che richiede un forte impegno alle aziende in nome di una maggiore tutela dei diritti degli interessati nel contesto dei servizi della società delle informazioni e delle reti, tutela tutta da verificare considerando che le soluzioni tecnologiche già in essere hanno una forza tale da imporre, nel frattempo che la proposta di regolamento procede nel suo iter di approvazione, standard de facto probabilmente ben diversi
- al di là degli intenti dichiarati, una capacità tutta da comprendere di essere in grado di fornire gli strumenti legali adeguati per un effettivo governo sul trasferimento di dati personali all'estero rispetto alla UE, realtà indiscussa per moltissimi servizi disponibili on line

Pertanto si attende che l'attuale processo di approvazione presso il Parlamento Europeo possa portare ad un regolamento che includa adempimenti ed obblighi effettivamente sostenibili ed attuabili a cura dei destinatari delle norme, nonché ad una reale maggior tutela per gli interessati.

2.4.2 La proposta di direttiva NIST

La “Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union” dell’8 Febbraio 2012 ha come principali obiettivi:

- la predisposizione di cooperazione e coordinamento tra gli enti europei competenti in materia di sicurezza delle informazioni
- la definizione di requisiti per la sicurezza e per i processi di intervento in caso di incidenti non solo per le cosiddette infrastrutture critiche ma per il ben più ampio contesto di sistemi delle pubbliche amministrazioni e degli “operatori di mercato”, tra i quali sono

  esplicitamente inclusi:

  - gli operatori on line (e-commerce, pagamenti on line, social networks, motori di ricerca, servizi di cloud computing, applicationstores)
  - operatori dei settori dell’Energia, Trasporto, Banche, Mercato finanziario, Aziende del settore sanitario

  esplicitamente escluse:

  - le microimprese e dunque secondo la regolamentazione EU le società con fatturato annuo inferiore a 2 milioni di euro e/o con meno di 10 dipendenti

Saranno di notevole impatto i requisiti di sicurezza posti a carico delle pubbliche amministrazioni e degli “operatori di mercato” interessati: dovranno predisporre misure di sicurezza individuate in base ad apposite analisi dei rischi e notificare alla autorità competente nazionale gli incidenti quando questi abbiano un impatto significativo sulla sicurezza dei servizi da loro erogati: è prevista anche la diretta comunicazione al pubblico nel caso in cui la rivelazione dell’incidente sia ritenuta da parte dell’autorità, di pubblico interesse. Tali requisiti di notifica di incidenti di sicurezza di fatto ampliano ad un numero potenzialmente assai elevato di soggetti le già esistenti obbligazioni di violazioni dati personali poste a carico degli operatori di servizi di comunicazioni elettroniche accessibili al pubblico, stabilite in particolare con la direttiva EU 2009/136/EC, recepita nel 2012 in Italia con i decreti legislativi 69 e 70.

È importante evidenziare che la proposta di direttiva NIS così come di fatto la proposta di nuova regolamentazione per la privacy descritta al paragrafo precedente, richiede che tali obbligazioni siano soddisfatte dagli operatori che forniscono servizi nella Unione Europea: questa espressione individua un contesto di destinatari ben più ampio delle aziende che sono stabilite in uno o più dei paesi membri UE in quanto suscettibile di includere anche le aziende, stabilite al di fuori della UE, che offrono servizi fruibili all’interno della Unione.

3.0 Contesto normativo italiano

La normativa italiana è in genere non poco frammentaria in materia di nuove tecnologie, vedasi anche le recenti ed evidenti problematiche per l'avvio di una effettiva operatività dell'Agenda Digitale italiana in linea con quella Europea. Ad oggi la normativa qui di interesse è rinvenibile in più atti normativi specifici per i vari contesti coinvolti, quali la tutela dei dati personali, la security, il cybercrime, la proprietà intellettuale, il commercio elettronico, le comunicazioni elettroniche.

3.1 Principali enti di riferimento

I provvedimenti aventi forza di legge vengono approvati in sede parlamentare, ma non mancano interventi di origine governativa sia nella forma di decreti legislativi sia genericamente di decreti. Non è raro leggere provvedimenti che riguardano la materia del "digitale" adottati, ad esempio, nella forma del decreto ministeriale che, per sua natura è un provvedimento amministrativo e non può prevalere rispetto ad altro avente forza di legge. I principali enti di riferimento sono indicati di seguito.

Il **Garante per la protezione dei dati personali** è un'autorità amministrativa indipendente istituita dalla cosiddetta legge sulla *privacy* ***(****legge 31 dicembre 1996, n. 675****)*** che ha attuato nell'ordinamento giuridico italiano la *direttiva comunitaria 95/46/CE* - e oggi disciplinata dal Codice in materia di protezione dei dati personali ***(****d.lg. 30 giugno 2003 n. 196****)***.

L'**Agenzia per l'Italia Digitale** è subentrata alla gestione della ex DigitPA, che prima ancora era CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione). L'Agenzia per l'Italia digitale è stata istituita con l'art. 19 del decreto-legge 22 giugno 2012, n. 83, convertito con modificazioni dalla L. 7 agosto 2012, n. 134. Le funzioni sono previste dall'art. 20 del medesimo decreto-legge; essa è preposta alla realizzazione degli obiettivi dell'Agenda digitale italiana, in coerenza con gli indirizzi elaborati dalla Cabina di regia di cui all'articolo 47 del decreto-legge 9 febbraio 2012, n. 5, convertito in legge con modificazioni dalla legge 4 aprile 2012, n. 35, e con l'Agenda digitale europea. In particolare l'Agenzia esercita le sue funzioni nei confronti delle pubbliche amministrazioni allo scopo di promuovere la diffusione delle tecnologie digitali nel Paese e di razionalizzare la spesa pubblica.

AGCOM. L'Autorità per le garanzie nelle comunicazioni è un'autorità indipendente, istituita dalla legge 249 del 31 luglio 1997. Indipendenza e autonomia sono elementi costitutivi che ne caratterizzano l'attività e le deliberazioni.Al pari delle altre autorità previste dall'ordinamento italiano, l'Agcom risponde del proprio operato al Parlamento, che ne ha stabilito i poteri, definito lo statuto ed eletto i componenti.

Nucleo per la sicurezza cibernetica. È stato istituito dal Decreto del Presidente del Consiglio dei Ministri 24 gennaio 2013, pubblicato in G.U. n. 66 del 19 marzo 2013.

3.2 Aspetti di interesse dalla normativa italiana vigente: focus on la violazione dei dati personali

Con i decreti legislativi n. 69 e n. 70 pubblicati in G.U. n. 126 del 31 maggio 2012 ed entrambi in vigore dal 1° giugno 2012, l'Italia ha recepito le direttive europee 2009/136/CE e 2009/140/CE in materia di telecomunicazioni, ed è stato così evitato il definitivo procedimento di infrazione previsto nei confronti di quegli Stati Membri che non hanno attuato entro i termini previsti i recepimenti di queste normative europee (era il 25 maggio 2011.

- Il **D.Lgs 70/12** modifica il D.Lgs 259/2003 - Codice delle comunicazioni elettroniche
- Il **D.Lgs 69/12** interviene sul D.Lgs 196/03 - Codice in materia di protezione dei dati personali (Codice Privacy), e su quest'ultimo porta le novità in materia di COOKIES ed in materia di VIOLAZIONE DEI DATI PERSONALI

Sono molte e tutte considerevoli le variazioni apportate al Codice Privacy (D.Lgs 196/03), espressamente per gli aspetti che riguardano la normativa in tema di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, in particolar modo con l'attuale titolo X "Comunicazioni elettroniche", artt.121-133, oltre l'art. 4 per quanto concerne le definizioni dei termini) nonché gli aggiornamenti per gli aspetti sanzionatori (art. 162-ter, art. 164-bis)

A seguito delle novità introdotte nel Codice Privacy con il D.Lgs 69/12, l'Autorità Garante per la protezione dei dati personali italiano ha prodotto a fine Luglio 2012 una prima Linea Guida in materia di violazione dei dati personali sottoposta a consultazione pubblica, e quindi emesso il provvedimento specifico con precisazioni riguardo:

- Tempistiche per le comunicazioni (notifiche) al Garante e se del caso agli utenti/altre persone
- Protocolli da osservare per le comunicazioni
- Misure di sicurezza

Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) - 4 aprile 2013*(Pubblicato sulla Gazzetta Ufficiale n. 97 del 4 aprile 2013)*

Riguardo la disciplina in materia di comunicazioni di violazioni dati personali, la Commissione Europea ha pubblicato il 26 Giugno 2013 un apposito Regolamento che **entra in vigore in tutti i paesi membri UE a partire dal 25 agosto 2013,** con lo scopo di stabilire regole comuni per tutti i paesi membri UE

"*L'esistenza di requisiti nazionali divergenti in proposito può dar luogo a incertezza giuridica, a procedure più complesse e gravose e a costi amministrativi considerevoli per i fornitori che operano a livello transfrontaliero. La Commissione ritiene pertanto necessario adottare le suddette misure tecniche di attuazione. ..Il presente regolamento riguarda esclusivamente la notifica delle violazioni di dati personali*"

REGOLAMENTO (UE) N. 611/2013 DELLA COMMISSIONE del 24 giugno 2013 sulle misure applicabili alla notifica delle violazioni di dati personali a norma della direttiva 2002/58/CE del Parlamento europeo e del Consiglio relativa alla vita privata e alle comunicazioni elettroniche", Gazzetta Ufficiale Europea n. 173, Giugno 26, 2013

L'impianto del Regolamento UE n. 611/2013 **non stravolge ma certamente comporterà adeguamenti** nel Provvedimento Data Breach del 4 aprile 2013 della Garante privacy italiano. L'Autorità infatti *"si riserva di intervenire nuovamente in merito ai tempi e al contenuto della comunicazione al Garante qualora nell'emanando Regolamento della Commissione relativo alle misure applicabili alla comunicazione delle violazioni di dati personali nell'ambito della Direttiva 2002/58/Ce sulla privacy e le comunicazioni elettroniche dovesse emergere un differente orientamento al riguardo."*

Per quanto concerne l'ambito soggettivo del Provvedimento del Garante in materia di data breach, ossia l'individuazione dei soggetti destinatari delle prescrizioni, è interessante qui evidenziarne gli aspetti principali, per le conseguenti ricadute in termini di aziende e contesti, per cui risulta necessario attivare (e mettere a budget…) processi ai fini degli adempimenti.

Essenzialmente il corpo delle prescrizioni è indirizzato ai

Fornitori= fornitori di servizi di comunicazione elettronica accessibili al pubblico

- *Al riguardo, anche al fine di individuare i soggetti interessati dalla nuova disciplina, si rinvia alle indicazioni fornite dal Garante con il provvedimento relativo alla "Sicurezza dei dati di traffico telefonico e telematico" (provv. del 17 gennaio 2008, pubblicato in G.U. n. 30 del 5 febbraio 2008, come modificato e integrato dal provvedimento del 24 luglio 2008, pubblicato in G.U. n. 189 del 13 agosto 2008), in quanto vi è una sostanziale identità dei titolari tenuti alla conservazione ex art. 132 del Codice, nonché all'adozione delle misure ivi prescritte con i destinatari della nuova disciplina ex art. 32-bis.*

- *In tale provvedimento, infatti, è stato evidenziato che "fornitori di servizi di comunicazione elettronica accessibili al pubblico" sono quei soggetti che realizzano esclusivamente, o prevalentemente, una trasmissione di segnali su reti di comunicazioni elettroniche, a prescindere dall'assetto proprietario della rete, e che offrono servizi a utenti finali secondo il principio di non discriminazione (cfr. anche direttiva 2002/21/Ce del Parlamento europeo e del Consiglio, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica -c.d. direttiva quadro- e d.lg. n. 259/2003 recante il Codice delle comunicazioni elettroniche).*

il Garante inoltre precisa che

- **non sono destinatari** delle prescrizioni: i soggetti che offrono servizi di comunicazione elettronica a gruppi delimitati di persone, titolari e gestori di esercizi pubblici che si limitano a mettere a disposizione del pubblico/clienti/soci telefoni o similari mezzi di comunicazione, i gestori di siti internet che diffondono esclusivamente contenuti, i gestori di motori di ricerca

- **sono invece ulteriori soggetti per le prescrizioni**:

  - i **gestori di siti internet** se offrono **servizi di posta elettronica e limitatamente a questi servizi**

  - **i servizi** di **mobile payment** con addebito e conseguente decurtazione del costo dal credito telefonico, per i clienti dotati di una carta di traffico telefonico ricaricabile, e con addebito sul conto telefonico per quelli che hanno l'abbonamento telefonico

Servizi erogati tramite altri soggetti

La nuova normativa prende espressamente in considerazione l'ipotesi in cui il Fornitore affidi l'erogazione del servizio di comunicazione elettronica ad altri soggetti.

In particolare, l'art. 32-bis, comma 8 D.Lgs 196/03, prevede che i soggetti esterni affidatari dell'erogazione del servizio siano tenuti a comunicare "senza indebito ritardo al fornitore tutti gli eventi e le informazioni necessarie a consentire a quest'ultimo di effettuare gli adempimenti" in materia di violazione dei dati personali.

Considerando ora tali **Affidatari**[15]dei servizi dei Fornitori

- Il Garante con il suo Provvedimento *Data Breach* fornisce in sostanza due **esempi** di Affidatari:
  - i fornitori di comunicazione elettronica tradizionali che erogano servizi ai MVNO (*Mobile Virtual Network Operator*)[16]
  - i soggetti terzi ai quali il Fornitore affida in tutto o in parte la materiale erogazione del servizio stesso, che hanno le infrastrutture a ciò necessarie, ad esempio per ragioni di ottimizzazione dei costi.
- in ogni caso **la realtà è come sempre più complessa:** tenendo presente la definizione di "Violazione di dati personali" occorrerà individuare con attenzione il soggetto Affidatario *tra*

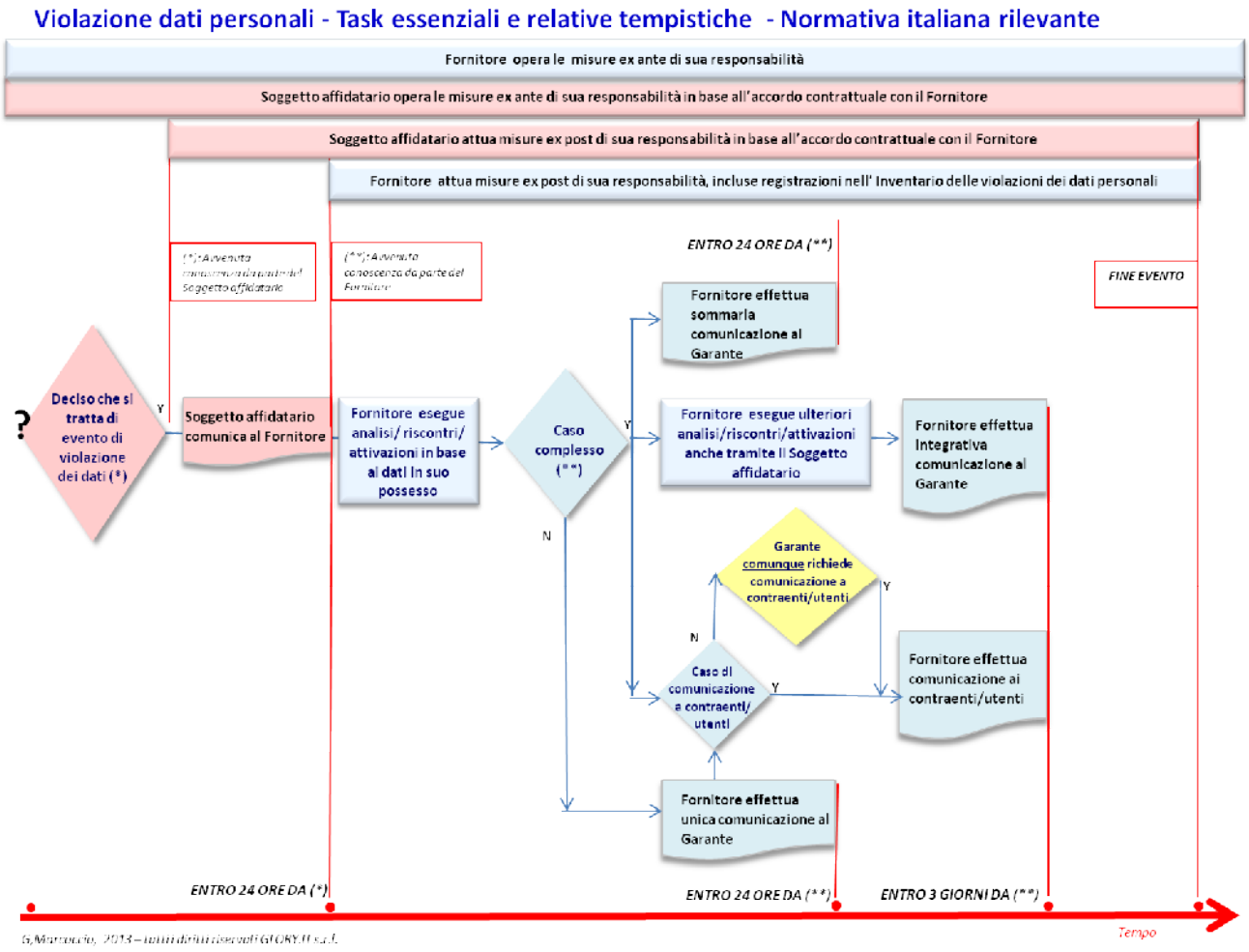
  quelle terze parti che il Fornitore coinvolge nel contesto della fornitura di un servizio di comunicazione elettronica accessibile al pubblico, i quali, in ragione del servizio erogato, siano nelle concrete condizioni di poter rilevare la violazione in luogo del Fornitore

Qui di seguito si riporta uno schema sintetico del provvedimento in oggetto allo scopo di evidenziare anche le azioni e le interattività che occorre tenere presenti quando i servizi sono erogati da Fornitore con il supporto, in tutto o in parte, di uno o più Affidatari dei servizi stessi

Si tenga presente che per quanto attiene alle tempistiche, ci si attende una operazione di revisione da parte del Garante allo scopo di assicurare la necessaria armonizzazione con quanto indicato nel provvedimento EU n. 611/2013.

[15] **Affidatario** qui si intende il soggetto a cui il Fornitore di un servizio di comunicazione elettronica accessibile al pubblico affida l'erogazione del predetto servizio, in tutto o in parte.

[16] Tipicamente si tratta di società che fornisce servizi di telefonia mobile senza possedere alcuna licenza per il relativo spettro radio né necessariamente avere tutte le infrastrutture necessarie per fornire tali servizi, utilizzando a tale scopo in tutto o in parte l'infrastruttura di un operatore mobile reale



Normativa di riferimento per lo schema:

- Modifiche al Codice Privacy a seguito del D.Lgs 69/12, in tema di violazione dei dati personali
- Provvedimento del Garante privacy in materia di violazione dei dati personali, 4 aprile 2013

4.0 Il punto di vista cloud

4.1 Aspetti di criticità

Da un punto di vista architetturale, nel contesto di servizi cloud, il trattamento di dati ai quali la legge e/o il loro titolare attribuisce valore e richiede determinate tutele, comporta controlli e misure di sicurezza diverse da quelle utilizzate quando i dati si trovavano nel perimetro aziendale: buona parte di queste misure di sicurezza consistono infatti nell'impedire l'accesso ai dati e quindi la fruizione di determinati servizi dal di fuori del perimetro aziendale stesso, implementando soluzioni di Network Security.

Con l'avvento del cloud, dunque, il perimetro aziendale si estende dal fruitore al fornitore del servizio e va quindi a comprendere sistemi e punti di accesso non più gestiti direttamente, rappresentando così un elemento di possibile ostacolo all'adozione di servizi in cloud nelle aziende.

Se per alcuni tipi di servizi più critici è ancora oggi sostenibile la gestione "in-house" ci sono tuttavia alcuni servizi che, man mano che evolvono, vengono ormai erogati esclusivamente in cloud e di cui molte organizzazioni non possono fare a meno – si pensi ad esempio ai servizi di Gestione Paghe e Amministrazione del Personale, piuttosto che ai servizi di gestione della forza vendita o ancora alla posta elettronica, fino ad arrivare a situazioni più complesse in cui il business aziendale richiede (ad esempio per una fase di test) di utilizzare una moltitudine di server virtuali che sarebbe decisamente anti-economico gestire "in-house".

Dunque, l'adozione di questi servizi obbliga a riflettere sul tema della protezione dei dati e della gestione della violazione degli accessi. Innanzi tutto, chi può accorgersi di una violazione? Occorre qui distinguere a seconda delle diverse tipologie di cloud:

- **Software-as-a-service**, ossia servizi "chiavi in mano" erogati tipicamente via web (come ad es. Salesforce.com): in questo caso è pressoché impossibile che sia l'amministratore IT dell'azienda cliente ad accorgersi di una possibile violazione, poiché non ha nessun tipo di accesso ai sistemi che erogano il servizio. L'amministratore IT dell'azienda cliente può quindi mettere in pratica alcuni accorgimenti per controllare gli accessi (di cui si parla nel paragrafo 5.3) ma non ha modo di sapere se i suoi dati vengono compromessi. Il fornitore del servizio cloud dovrebbe quindi essere tenuto a comunicare l'avvenuta violazione all'azienda cliente che, a cascata, a seconda del tipo di dato compromesso, potrebbe essere tenuta a inviare la comunicazione ai singoli titolari dei dati. Un esempio pratico è rappresentato dalla posta elettronica che il provvedimento del Garante del 4 Aprile 2013 chiaramente include tra i casi soggetti a tutela anche se il servizio è fornito da un content provider oltre che dai forntiori di servizi tlc/internet – in questo caso ad esempio, il contratto dovrebbe ritenere l'azienda cliente responsabile dell'accesso alle singole caselle e il provider responsabile dell'accesso ai sistemi che erogano il servizio e la cui compromissione potrebbe portare all'accesso illegittimo a più caselle contemporaneamente.

- **Platform-as-a-service**, ossia una piattaforma su cui l'azienda cliente costruisce i propri servizi sfruttando un livello di astrazione fornito dal cloud provider. In questo caso possono accorgersi di una violazione sia il cloud provider (che controlla ad esempio gli accessi a sistema operativo, DB ecc.) sia il cliente (che controlla l'accesso alle applicazioni). Da un punto di vista contrattuale è quindi importante definire bene la matrice delle responsabilità e il livello di sicurezza atteso. Un esempio pratico è rappresentato dai servizi di Mobile Payment, a cui il Garante ha esteso la normativa: il provider è tenuto a comunicare l'avvenuta violazione ma in realtà il servizio si appoggia su un'infrastruttura gestita da terzi e su cui ha un controllo molto limitato.

- **Infrastructure-as-a-service**, ossia l'utilizzo di server virtuali gestiti in tutto e per tutto dal cliente finale: in questo caso è principalmente l'amministratore IT dell'azienda cliente che controlla l'accesso ai dati e agli ambienti virtuali. Un caso in cui risulta esservi responsabilità da parte del provider appare essere l'eventualità del furto di copie degli ambienti virtuali, che altro non sono che semplici file immagazzinati sui dischi del provider. Per ovviare a questo problema possono essere implementate misure quali quelle descritte nella sezione 5.3, che consentono di tenere in house lato cliente il controllo completo della propria infrastruttura, anche se si trova in cloud.

Un secondo aspetto che deve essere tenuto in considerazione è la distribuzione geografica dei dati: alcune informazioni devono infatti, per legge, risiedere in Italia o almeno nella Comunità Europea a meno di adozioni di particolari strumenti legali per legittimarne il trasferimento all'estero e questo rappresenta un altro serio ostacolo all'adozione di servizi cloud.

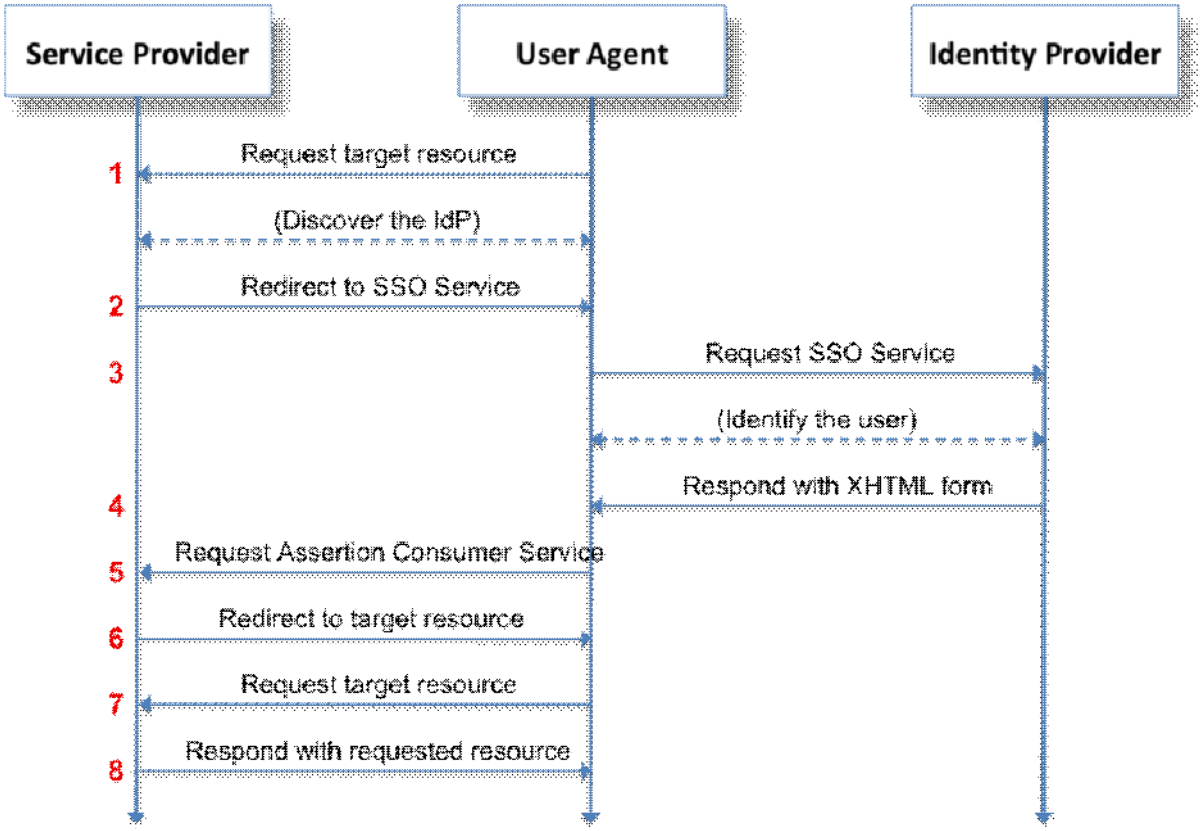
Una possibile base tecnica per la soluzione, di cui si parla nei successivi paragrafi, è rappresentata dalla cifratura dei dati eseguita con chiavi che risiedano fisicamente in un sistema dedicato, localizzato in Italia – questo rende i dati che risiedono all'estero inutilizzabili e inintelleggibili contribuendo così ad agevolare l'adozione di servizi cloud.

4.3 Possibili misure tecnico/organizzative

In questo capitolo analizziamo alcune soluzioni tecniche e misure organizzative che possono aiutare le aziende a gestire in sicurezza i servizi in cloud, tenendo presente nel complesso le misure tecniche ex ante ed ex post che devono comunque essere predisposte ai fini della minimizzazione del rischio di data breach.

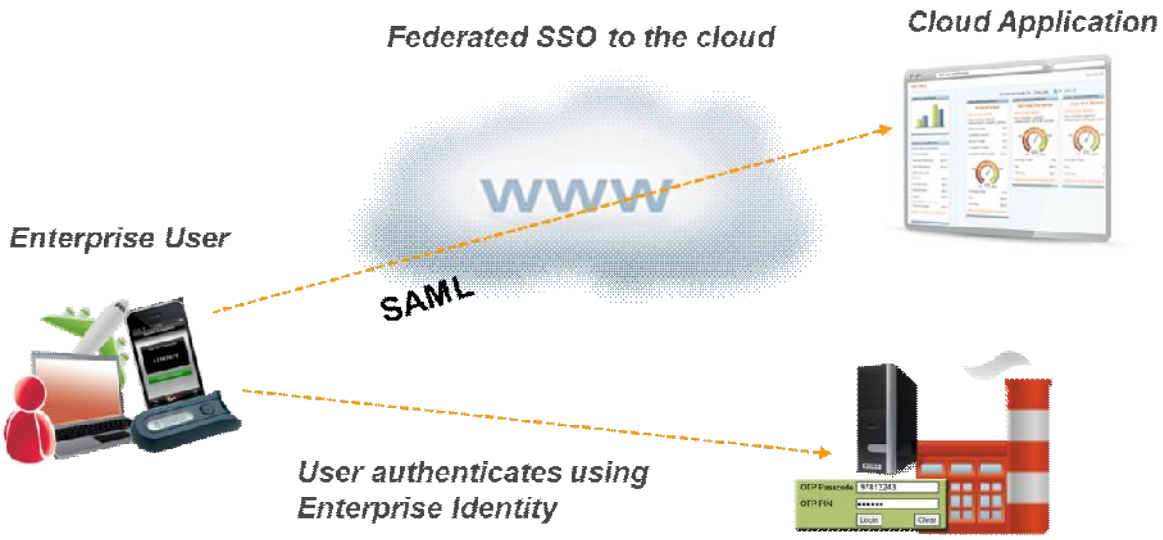
4.3.1 Autenticazione degli utenti

Accedere a servizi in cloud potrebbe voler dire trasferire in cloud anche la gestione degli accessi ma è chiaro che questo pone diversi problemi organizzativi e tecnici (ad esempio, chi si preoccupa di disabilitare l'utenza di chi lascia l'azienda?). Per questo è stato standardizzato il protocollo SAML (acronimo di Security Assertion Markup Language) per gestire le identità verso i servizi cloud facendo si che l'utente venga autenticato da un server on-premises e poi re-diretto al servizio cloud.



Nel caso di Software-as-a-service, però, da un punto di vista di sicurezza come abbiamo visto al paragrafo precedente l'azienda non ha nessun controllo sulle piattaforme che erogano i servizi e di conseguenza non può nemmeno accorgersi se uno o più account vengono violati – un problema ancora più evidente se si pensa che questi servizi sono liberamente accessibili da Internet.

Per questo motivo le principali soluzioni di autenticazione a due fattori (o Strong Authentication) sul mercato sono evolute per supportare il protocollo SAML e quindi garantire un effettivo controllo degli accessi da parte dell'azienda: per accedere al servizio non basta più infatti conoscere (o indovinare...) una password ma è necessario avere un token che può essere un oggetto hardware o un client da installare sul proprio smartphone.



Alcuni player nel settore della strong authentication, come SafeNet, erogano poi dal cloud il servizio di Strong Authentication – ma in questo caso, trattandosi di un servizio di sicurezza, il controllo è in mano all'azienda e semplicemente si evita di dover gestire un'infrastruttura in casa propria, automatizzando il più possibile la gestione del servizio.

4.3.2 Protezione dei dati in Cloud

Come riportato precedentemente, uno dei temi più importanti nell'utilizzo di servizi cloud è il controllo sui dati che vengono salvati presso il fornitore del servizio, principalmente per questi motivi:

- La normativa italiana prevede l'obbligo di comunicazione, verso il Garante privacy ed in alcuni casi verso i contraenti ed altri individui, in caso violazione dei dati personali nel settore delle telecomunicazioni e di altre categorie "assimilate" come ad esempio i fornitori di servizi di Mobile Payment
- In alcuni contesti vige l'obbligo di custodire i dati nel territorio dell'Unione Europea
- Gli amministratori di sistema del fornitore di servizi potrebbero accedere liberamente ai dati e di conseguenza utilizzarli per scopi illeciti senza che l'azienda cliente se ne renda conto
- Al termine del contratto con un fornitore è importante avere garanzia che i dati che ancora risiedono nella sua infrastruttura vengano cancellati – questa garanzia aiuta anche a minimizzare il cosiddetto "lock-in" cioè la difficoltà o impossibilità di cambiare fornitore

Per tutti questi scenari, una possibile soluzione è rappresentata dalla cifratura dei dati: in questo caso, se anche i dati venissero in qualche modo copiati in modo non autorizzato sarebbero comunque inutilizzabili perché l'azienda cliente custodisce le chiavi necessarie per decifrarli. Il tema quindi non è più soltanto cercare di impedire che la perdita di informazioni avvenga – perché come abbiamo detto in ottica cloud difendere il perimetro è ormai impossibile – ma è, piuttosto, mettersi nella condizione in cui un possibile "breach" non abbia conseguenze.

A seconda del tipo di servizio Cloud esistono diversi modi per raggiungere questo obbiettivo:

- Software-as-a-service: questo è il caso più difficile da gestire, poiché l'infrastruttura è completamente in mano al fornitore del servizio. Esistono quindi sul mercato diverse soluzioni che cifrano i dati prima che vengano salvati presso il provider, come ad esempio CipherCloud – basandosi però su un gateway da installare presso il cliente. Tali soluzioni devono essere valutate con attenzione perché significa veicolare tutto il traffico attraverso la propria infrastruttura, cosa che di solito utilizzando un servizio in Cloud non si desidera.
- Platform-as-a-service: in questo caso l'applicazione può implementare la cifratura dei dati. Da un punto di vista di sicurezza è però importante che le chiavi di cifratura non risiedano nell'applicazione stessa perché questo vanificherebbe l'utilità di cifrare. Una possibilità è quindi quella di utilizzare un sistema esterno a cui demandare la custodia delle chiavi di cifratura, la loro gestione (controllo accessi, rotazione, ciclo di vita...) ed eventualmente anche le operazioni di cifratura e decifratura (in questo modo le chiavi non uscirebbero mai dal sistema sicuro). Anche in questo caso esistono sul mercato diverse possibilità come ad esempio SafeNetDataSecure che è una piattaforma sicura di encryption e key management disponibile sia in versione hardware che in versione virtualappliance, adatta a implementazioni in Cloud.
- Infrastructure-as-a-service: in questo caso l'accesso ai sistemi operativi è regolato direttamente dal cliente del servizio cloud. E' quindi importante proteggersi soprattutto dall'eventualità che il fornitore di servizi possa copiarsi i dati "a riposo" ossia le macchine virtuali e i dischi virtuali – copiare un server su una chiavetta USB è infatti oggi un'operazione di pochi secondi, decisamente più

semplice di quanto fosse effettuare la copia di un server fisico. In questo caso esistono sul mercato almeno due soluzioni – TrendMicroSecureCloud e SafeNetProtectV – per cifrare le macchine virtuali vmware e istanze Amazon WebServices e, nel caso di ProtectV, anche le partizioni di avvio, il che garantisce la massima sicurezza ai sistemi virtuali.

Riepilogando dunque la crittografia rappresenta sicuramente un valido aiuto per la migrazione verso servizi in cloud e risponde al criterio di "inintellegibilità" dei dati ribadito dal Garante Privacy con il suo intervento in materia di data breach– il che significa sostanzialmente che la violazione di dati personali cifrati non dovrà essere comunicata obbligatoriamente entro i termini stabiliti dalla legge ai contraenti ed altri individui soggetti alla violazione. Inoltre la crittografia può supportare da un punto di vista tecnico la soluzione al problema della localizzazione dei dati all'interno dell'Unione Europea nel momento in cui le chiavi di encryption sono custodite in un hardware dedicato installato in Italia, perché i dati sono inutilizzabili senza le chiavi. Resta comunque importante per un'azienda creare un processo di gestione delle violazioni di accesso ai dati e costruire un inventario, ovviamente cifrato, per rispondere ai requisiti di legge.

4.3.3 Gestione degli Eventi

Nei paragrafi precedenti abbiamo spesso fatto riferimento all'obbligo, per i diversi soggetti coinvolti in un'architettura Cloud, di accorgersi e quindi gestire le violazioni di accesso ai dati. L'evoluzione delle architetture e la progressiva dissoluzione del perimetro aziendale, tuttavia, rende complicato accorgersi di anomalie analizzando manualmente i log di ciascuna sorgente (es. Firewall, database ecc.) – tra l'altro spesso le anomalie sono rappresentate da qualcosa che non c'è, e dunque è impossibile notarle senza guardare contemporaneamente a più fonti (ad esempio, l'accesso a un database che non passa da un firewall potrebbe indicare un accesso illegittimo dall'interno della rete aziendale).

Per analizzare gli eventi di sicurezza in modo integrato esistono dunque sul mercato i cosiddetti sistemi SIEM, acronimo di Security Information and Event Management. Questi sistemi sono dunque il punto centrale per raccogliere, salvare, analizzare e generare allarmi a partire dai log per rispondere a un incidente, per analizzare l'accaduto e per essere in regola con le norme di compliance.

Tra i sistemi SIEM più noti sul mercato troviamo ad esempio QRadar di IBM, ArcSight di HP, l'Enterprise Security Manager di McAfee insieme a diversi altri.

Un punto di attenzione è ovviamente la gestione delle informazioni raccolte da questi sistemi, perché possono essere esse stesse informazioni sensibili e comunque devono essere custodite in modo sicuro e in modo che non siano modificabili – a maggior ragione se questi dati vengono salvati su una porzione di infrastruttura condivisa con altri dipartimenti o gestita da terzi, come nel caso di outsourcing e di cloud. Per questo è possibile utilizzare due approcci, complementari tra loro:

- Full Disk Encryption, ossia cifratura dei dischi a basso livello: questa tecnica protegge sostanzialmente dal furto fisico dei dischi e dai problemi derivanti da un possibile accesso non autorizzato ai dati in caso i dischi vengano mandati in riparazione o sostituiti. Una volta "sbloccato" un disco, infatti, i dati sono in chiaro e non c'è un controllo degli accessi granulare. Quasi tutti i vendor di sistemi di Storage offrono questa funzionalità.
- Cifratura delle share su cui risiedono i dati: in questo caso, vengono cifrati proprio i dati, il che significa che chiunque voglia visualizzarli dovrà essere autorizzato. Si realizza cosi un sistema di controllo accessi in linea, trasparente per gli utenti autorizzati ma bloccante per i tentativi di accesso non autorizzati. Questo è un approccio innovativo che punta a proteggere il dato ed è stato implementato, tra i primi, dal sistema Decru, acquisito da NetApp e oggi diventato SafeNetStorageSecure.

Appendice 1 - Servizi di comunicazione elettronica accessibili al pubblico e Normativa italiana Data Breach Aspetti inerenti le misure contrattuali tra i soggetti destinatari delle prescrizioni

Introduzione

Questa nota fornisce una panoramica degli aspetti da tenere presenti relativamente alla documentazione contrattuale tra i soggetti coinvolti nell'erogazione di servizi di comunicazione elettronica accessibili al pubblico, alla luce delle nuove prescrizioni in materia di violazione dei dati personali, conseguenti al recepimento in Italia della direttiva europea 2009/136/CE.

Contesto prescrittivo di riferimento

Il recepimento di interesse in materia di violazione dei dati personali (*data breach)* è avvenuto tramite il D.Lgs 69/12 che ha modificato in modo significativo il D.Lgs 196/03, relativamente al trattamento dei dati personali e tutela della vita privata nel settore dei servizi delle comunicazioni elettroniche accessibili al pubblico su reti pubbliche di comunicazione.

Le modifiche di interesse al D.Lgs 196/03 (Codice Privacy) riguardano i seguenti articoli:

- art. 4, comma 3, punto g-bis) - (aggiunto *ex novo:* introdotta la definizione di "violazione di dati personali")
- a**rt. 32 "Obblighi relativi ai fornitori di servizi di comunicazione elettronica accessibili al pubblico" (articolo relativo alla sicurezza nei servizi, modificato in più punti in modo sostanziale)**
- **art. 32-bis "Adempimenti conseguenti ad una violazione di dati personali" (aggiunto *ex novo*)**
- **art. 132-bis "**Procedure istituite dai fornitori" (aggiunto *ex novo*: sebbene non direttamente connesso alla *data breach* questa prescrizione si considera comunque rilevante ai fini dei rapporti contrattuali tra i soggetti coinvolti nei servizi qui di interesse)
- **art. 162-*ter "S*anzioni nei confronti di fornitori di servizi di comunicazione elettronica accessibili al pubblico" (aggiunto *ex novo*)**
- **art. 168 "Falsità nelle dichiarazioni e notificazioni al Garante" (modificato)**

L'Autorità Garante per la protezione dei dati personali ha quindi adottato un apposito provvedimento generale per specificare gli adempimenti previsti in materia di *data breach*: "Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach)", in conseguenza del comma 6 dell'art. 32-bis, che riconosce al Garante la facoltà di emanare orientamenti ed istruzioni in relazione alle circostanze in cui vi è obbligo di comunicazione delle *data breach*, il formato applicabile a tali comunicazioni nonché le relative modalità di effettuazione.

Inoltre, a partire dal 25 agosto 2013 entra in vigore direttamente anche in Italia (così come in tutti i paesi Membri UE) la Regolamentazione UE in materia di comunicazioni delle violazioni dei dati personali:

"REGOLAMENTO (UE) N. 611/2013 DELLA COMMISSIONE del 24 giugno 2013 sulle misure applicabili alla notifica delle violazioni di dati personali a norma della direttiva 2002/58/CE del Parlamento europeo e del Consiglio relativa alla vita privata e alle comunicazioni elettroniche"

Definizioni, acronimi e posizioni

Ai fini di questa nota per:

- **Garante** si intende l'Autorità Garante per la protezione dei dati personali
- **Provvedimento Data Breach** si intende il provvedimento del Garante "Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach)"
- **Fornitore** si intende il fornitore di un servizio di comunicazione elettronica accessibile al pubblico, essenziale destinatario della normativa qui di interesse. Questo termine potrebbe portare qualche difficoltà nel leggere alcune parti nei prossimi paragrafi relativamente alla documentazione contrattuale, in quanto tale Fornitore è nel contesto qui trattato la "parte acquirente" di un servizio fornito da una "parte fornitrice". Si è comunque preferito mantenere il termine Fornitore in quanto è quello utilizzato nelle prescrizioni di legge qui di interesse. Laddove l'uso del termine Fornitore è sembrato troppo fuorviante nell'ambito descrittivo, in suo luogo è stato utilizzato il termine di "parte acquirente"
- **Affidatario** si intende il soggetto a cui il Fornitore di un servizio di comunicazione elettronica accessibile al pubblico affida l'erogazione del predetto servizio, in tutto o in parte. Laddove l'uso di tale termine è sembrato non chiaro nell'ambito descrittivo, in suo luogo è stato utilizzato il termine di "parte fornitrice"
- **Responsabile ex art. 29** si intende il responsabile del trattamento dati personali ai sensi dell'art. 29
- ***Data Breach*** si intende la violazione dei dati personali, ai sensi dell'art. 4, comma 3, punto g-bis) al D.Lgs. 196/03.

Laddove non specificamente indicato, gli **articoli menzionati nel testo sono sempre riferiti al D.Lgs. 196/03.**

I soggetti coinvolti nel rapporto contrattuale

Il Fornitore (la parte acquirente)

La normativa qui di interesse è essenzialmente indirizzata ai fornitori di servizi di comunicazione elettronica accessibili al pubblico, intendendo per essi *"quei soggetti che realizzano esclusivamente, o prevalentemente, una trasmissione di segnali su reti di comunicazioni elettroniche, a prescindere dall'assetto proprietario della rete, e che offrono servizi a utenti finali secondo il principio di non discriminazione*[17]*"*, come già espresso dal Garante in occasione del suo provvedimento relativo alla "Sicurezza dei dati di traffico telefonico e telematico"[18].

In questo contesto, il Garante con il suo Provvedimento *Data Breach* al paragrafo 3 "Ambito soggettivo" precisa che

- **non sono destinatari** delle prescrizioni: i soggetti che offrono servizi di comunicazione elettronica a gruppi delimitati di persone (quali ad esempio le aziende pubbliche e private nei riguardi dei servizi di comunicazioni interne), titolari e gestori di esercizi pubblici che si limitano a mettere a disposizione del pubblico/clienti/soci telefoni o similari mezzi di comunicazione, i gestori di siti internet che diffondono esclusivamente contenuti (content provider), i gestori di motori di ricerca
- **sono invece ulteriori soggetti per le prescrizioni**:

[17] *cfr. anche direttiva 2002/21/Ce del Parlamento europeo e del Consiglio, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica -c.d. direttiva quadro- e d.lg. n. 259/2003 recante il Codice delle comunicazioni elettroniche*

[18] *provv. del 17 gennaio 2008, pubblicato in G.U. n. 30 del 5 febbraio 2008, come modificato e integrato dal provvedimento del 24 luglio 2008, pubblicato in G.U. n. 189 del 13 agosto 2008*

- anche i gestori di siti internet ma se offrono servizi di posta elettronica e limitatamente a questi servizi
- i servizi di mobile payment con addebito e conseguente decurtazione del costo dal credito telefonico, per i clienti dotati di una carta di traffico telefonico ricaricabile, e con addebito sul conto telefonico per quelli che hanno l'abbonamento telefonico

L'Affidatario (la parte venditrice)

L'Affidatario è quel soggetto al quale il Fornitore affida in tutto o in parte l'erogazione di uno o più servizi di comunicazione elettronica accessibile al pubblico. Il Garante con il suo Provvedimento *Data Breach* al paragrafo 3.1"Servizi erogati tramite altri soggetti" fornisce in sostanza due esempi di Affidatari:

- i fornitori di comunicazione elettronica tradizionali i quali offrono ed erogano i servizi ad esempio alle società che forniscono servizi di telefonia mobile senza possedere alcuna licenza per il relativo spettro radio né tutte le infrastrutture necessarie per fornire tali servizi (MVNO - Mobile Virtual Network Operator)[19]
- i soggetti terzi ai quali il Fornitore affida in tutto o in parte la materiale erogazione del servizio stesso, che hanno le infrastrutture a ciò necessarie, ad esempio per ragioni di ottimizzazione dei costi.

Questi esempi sono estremamente importanti e rappresentativi di una elevatissima percentuale dei casi reali di rapporto Fornitore – Affidatario: in ogni caso la realtà è come sempre più complessa e dinamica per cui non sembra agevole farla rientrare sempre e pienamente in qualunque tentativo di schematizzazione. Per cui, tenendo presente la definizione di "Violazione di dati personali" occorrerà individuare il soggetto Affidatario tra quelle terze parti che il Fornitore coinvolge nel contesto della fornitura di un servizio di comunicazione elettronica accessibile al pubblico, i quali, in ragione del servizio erogato, siano nelle concrete condizioni di poter rilevare la violazione in luogo del Fornitore.

Da ricordare infine che la normativa oggetto di questa nota **non modifica in alcun modo** quanto attiene alla eventuale nomina dell'Affidatario come Responsabile ex art 29 del Fornitore: occorrerà quindi che il Fornitore e l'Affidatario, nello specifico contesto del servizio oggetto della relazione contrattuale, configurino i loro ruoli in termini di titolare e responsabile del trattamento, tenendo presente che, ai sensi del D.Lgs 196/03 (art. 4 comma lettere f) e g) e art. 29):

- il titolare è "*la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza",*
- il responsabile è *"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali"*;
- il titolare designa facoltativamente il responsabile: in caso di designazione il titolare fornisce al responsabile le istruzioni a cui attenersi ed effettua controlli, anche periodici, sul suo operato.

[19] *Come specificato dal Garante "I MVNO sono dotati di archi di numerazione telefonica propri e quindi di proprie SIM card, possono gestire in proprio le funzioni di commutazione e di trasporto nonché la base dati di registrazione degli utenti mobili. Sono, quindi, completamente autonomi nella relazione con i clienti, i quali non hanno alcun rapporto diretto con l'operatore di rete mobile e stipulano un unico contratto, appunto, con il MVNO."*

Note per gli aggiornamenti contrattuali da considerare

Alla luce dell'evoluzione normativa sopra brevemente richiamata, si prospetta l'esigenza di integrare la documentazione contrattuale tra Fornitore e Affidatario, in termini di aggiornamenti delle clausole contrattuali che riguardano l'approntamento di misure di sicurezza e obblighi di comunicazione in caso di *Data Breach*, incluse relative penali/sanzioni in caso di violazione di tali clausole e della eventuale nomina a Responsabile ex art. 29 incluse le relative istruzioni. In considerazione delle nuove prescrizioni in materia di *Data Breach* la documentazione contrattuale tra Fornitore (Parte acquirente) ed Affidatario (Parte venditrice) contemplerà elementi in grado di circoscrivere gli obblighi in relazione a:

- approntamento delle misure di sicurezza ex ante ed ex post rispetto alle violazioni di dati personali
- comunicazioni in caso di violazioni dati personali

e prevedere

- penali in caso di violazione di tali obblighi
- aggiornamento della clausola risolutiva espressa

Solo allo scopo di fornire un filo conduttore, in quanto le effettive clausole dovranno tener conto dello specifico contesto di riferimento del servizio (nuovo, già esistente, già identificato o meno come soggetto alle prescrizioni in materia di *Data Breach*,…) è indicata qui di seguito una struttura articolata su 4 set di requisiti ai quali trovare riscontro nel corpo della documentazione contrattuale.

1) Misure di sicurezza e *governance* di accesso ai dati

Nel rispetto e per i fini della normativa in materia di violazione dati personali: gli artt. 4 co. 3 punto g-bis, 32 e 32-bis, 132-bis del D.Lgs. 196/03, Provvedimento dell'Autorità garante per la protezione dei dati personali in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. *data breach*) del 4 aprile 2013, G.U. 97/13, e successive modifiche ed integrazioni anche in relazione al Regolamento EU n. 611/2013l'Affidatario avrà l'obbligo di:

- approntare le misure di sicurezza
  - adeguate al rischio esistente per salvaguardare la sicurezza dei servizi oggetto del Contratto
  - per prevenire l'insorgenza di violazioni dei dati personali
  - per limitare gli effetti pregiudizievoli in caso di avvenuta violazione di dati personali
- consentire l'accesso ai dati personali soltanto a personale autorizzato per fini legalmente autorizzati che necessita di operare sulle reti di comunicazione elettronica per i servizi oggetto del Contratto
- informare prontamente il Fornitore (Parte Acquirente), qualora riceva una qualunque richiesta di accesso ai dati personali degli utenti del Fornitore stesso

2) Obblighi di comunicazione in caso di violazione di dati personali

Nel rispetto e per i fini della normativa in materia di violazione dati personali: gli artt. 4 co. 3 punto g-bis, 32 e 32-bis del D.Lgs. 196/03, Provvedimento dell'Autorità garante per la protezione dei dati personali in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. *data breach*) del 4 aprile 2013, G.U. 97/13, e successive modifiche ed integrazioni, anche in relazione al Regolamento EU n. 611/2013,l'Affidatario, in caso di violazione dei dati personali, avrà l'obbligo di comunicare al Fornitore senza indebito ritardo detta violazione , dalla avvenuta conoscenza:

- comunque entro i limiti temporali previsti dalla normativa applicabile

- indicandone tutti gli eventi e le informazioni necessarie a consentire al Fornitore stesso di effettuare gli adempimenti previsti all'art 32-bis del D.Lgs 196/03

3) Penale in caso di violazione degli obblighi di cui ai precedenti punti 1) e 2)

Occorre tenere presente che la modifica legislativa che ci occupa ha introdotto un nuovo articolo 162-ter *"Sanzioni nei confronti di fornitori di servizi di comunicazione elettronica accessibili al pubblico"*, con il quale sono previste sanzioni particolarmente gravose per la violazione dell'art. 32-bis "Adempimenti conseguenti una violazione di dati personali", come riportato nella seguente tabella riepilogativa.

VIOLAZIONE	SANZIONE
art. 32-bis co. 1 (Omessa comunicazione di violazione dati personali al Garante)	fino a €. 150.000
art. 32-bis co. 2 (Omessa comunicazione di violazione dati personali al contraente o altre persone)	fino a €. 1.000 per ciascuna persona nei cui confronti venga omessa o ritardata la comunicazione prevista; il tutto fino alla misura massima del 5% del volume d'affari realizzato dal fornitore di servizi
art. 32-bis co. 7 (Violazione della disposizione concernente la tenuta di un aggiornato inventario delle violazioni dei dati personali)	fino a €. 120.000
Le medesime sanzioni "si applicano nei confronti dei soggetti a cui il fornitore di servizi di comunicazione elettronica accessibili al pubblico abbia affidato l'erogazione dei predetti servizi, qualora tali soggetti non abbiano comunicato senza indebito ritardo, al fornitore, ai sensi dell'articolo 32-bis, comma 8, le informazioni necessarie ai fini degli adempimenti di cui all'articolo 32-bis."	

Inoltre la modifica legislativa ha riguardato l' art. 168 "Falsità nelle dichiarazioni e notificazioni al Garante", che prevede ora la sanzione penale della reclusione fino a tre anni, salvo che il fatto costituisca più grave reato, anche nel caso delle comunicazioni di violazione di dati personali da Fornitore verso il Garante (art.32-bis co.1) e da Affidatario verso il Fornitore (art. 32-bis co.8).

Pertanto si ipotizza che nel corpo della documentazione contrattuale debba essere prevista una clausola penale per mantenere indenne il Fornitore da eventuali oneri e/o spese sostenuti a seguito di obblighi disattesi dall'Affidatario.

4) **Aggiornamento della clausola risolutiva espressa**

Da ultimo, poiché le conseguenze dannose derivanti da una violazione degli obblighi di legge qui di interesse potrebbero comportare un danno diretto (economico) o indiretto (danno d'immagine), attesa la gravità delle sanzioni previste dalla legge e sopra richiamate, appare opportuno introdurre un articolo che inserisca la possibilità di una risoluzione anticipata del contratto (mediante una clausola risolutiva espressa ex art. 1456 c.c.), da azionare nel caso in cui gli eventi di violazioni corrispondano ad un determinato criterio che, a titolo esemplificativo potrebbe consistere nella reiterazione della violazione degli obblighi di cui ai punti 1) e 2) precedenti.

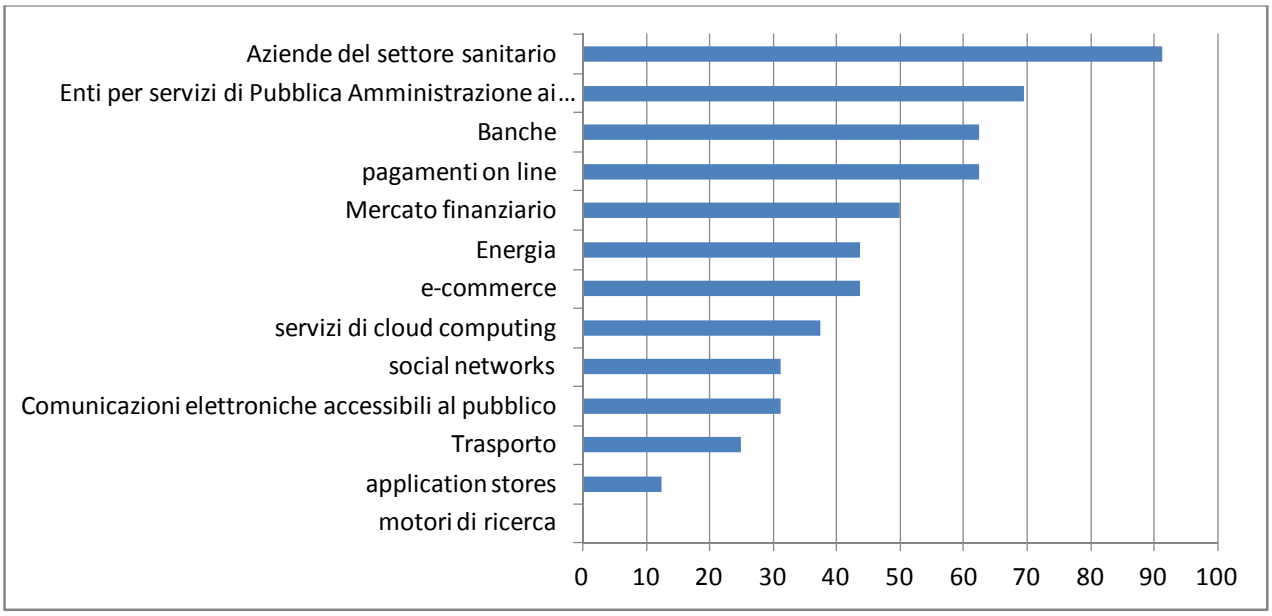
Integrazione alla nomina a Responsabile ex art 29 d.Lgs 196/03

Sebbene i nuovi obblighi a carico dell'Affidatario, in conseguenza degli aggiornamenti normativi qui di interesse, siano validi indipendentemente dalla eventuale nomina dell'Affidatario quale Responsabile ex art. 29 del Fornitore, appare opportuno di conseguenza integrare la eventuale nomina e le relative istruzioni ai sensi dell'art- 29 D.Lgs 196/03.

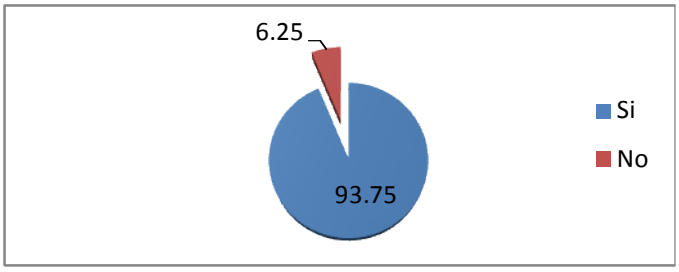
Appendice 2 - Risultati della Survey:Data breach in the cloud □ partecipa alla CSA Italy chapter survey, conclusa il 10 maggio 2013

Tutti i valori numerici presentati nei grafici sono espressi in termini percentuali

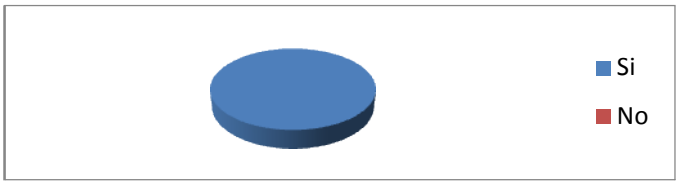
1) In quale settore ritieni più pericoloso il caso di violazione di dati per servizi erogati in modalità cloud



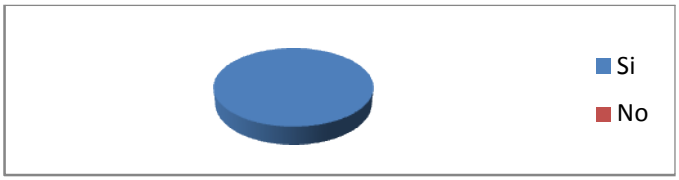
2)Ritieni che sia importante per un utente finale di un servizio erogato in modalità cloud sapere, in caso di comunicazione a lui diretta di avvenuta violazione di dati, dove (localizzazione geografica) e a responsabilità di quale sub-provider è avvenuta la violazione?



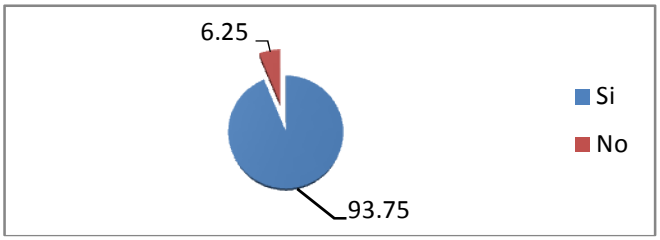
3) In caso di violazione ritieni che sia importante che l'utente finale venga a sapere come si è conclusa la violazione, quali rimedi sono stati adottati ed a cura di chi (sorta di breve rendicontazione)?



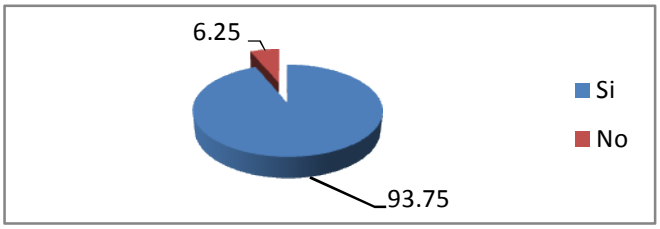
4) Ritieni che per l'utente finale/per le autorità competenti/altri stakeholder sia utile l'istituzione di un data base che raccolga le informazioni su eventi di violazione dei dati avvenute, comprensive di una minima circostanzi azione in termini di: che tipo di violazione, chi l'ha causata e come, quali enti ne sono stati coinvolti?



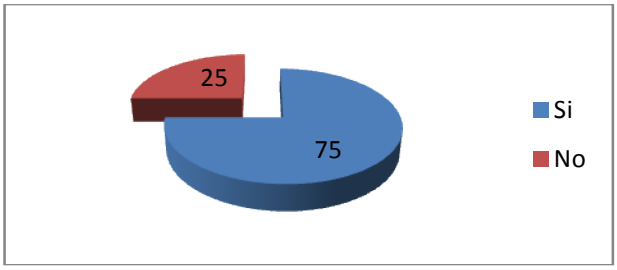
5) Ritieni utile che il numero/tipologia di violazioni di dati avvenute in un dato intervallo di tempo debba diventare una sorta di KPI (Key Performance Indicator) pubblico, messo a disposizione a cura del cloud provider, come forma di trasparenza ma anche di autocontrollo per la qualità del servizio offerto?



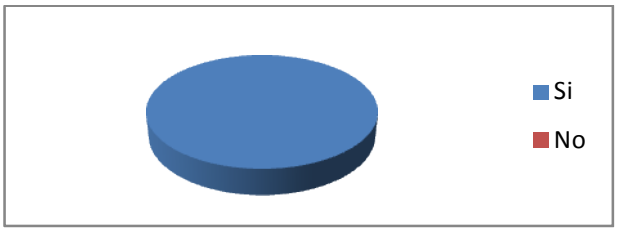
6) Ritieni che sia utile un coordinamento su questo tema tra più paesi, almeno appartenenti ad una area geo-politica?



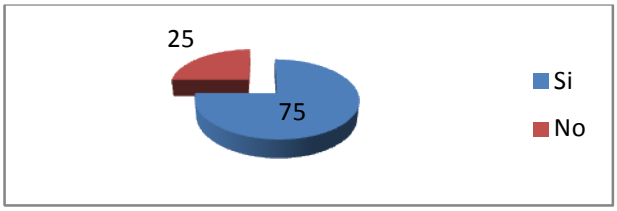
7) Ritieni che sarebbe utile predisporre un coordinamento simile al precedente ma a livello di associazioni/organizzazioni di confederazione tra gli operatori di un dato settore?



8) Ritieni che per trasparenza e per un effettivo livello di protezione dei dati e di autocontrollo i cloud computing provider tramite una associazione/organizzazione di settore debbano pubblicare periodicamente dati in merito alle violazioni di dati occorse nei loro servizi?



9) Saresti disposto a pagare un servizio, ora fruito gratuitamente, pur di avere certezza che vi sia un apparato di governo e controllo contro le violazioni di dati, in termini di appropriate misure di sicurezza?



10) Vuoi indicarci uno o più aspetti che a tuo avviso debbano essere messi in luce in una analisi del tema violazione dati nel contesto cloud computing?

(questa era una domanda di carattere puramente facoltativo: le risposte ottenute sono elencate qui di seguito)

RISPOSTA 1

sarebbe utile arrivare a determinare in dettaglio quali informazioni sono state sottratte o modificate quali sono i tenant sicuramente coinvolti nella violazione, quali sono in posizione dubbia e quali non sono stati affetti dalla violazione i termini in cui la violazione si è perpetrata quali sono le circostanze favorevoli che hanno permesso la violazione

RISPOSTA 2

la gestione dell'incidente e la trasparenza nei confronti dell'utente finale della violazione. Quest'ultimo punto è molto importante, secondo me, perché solo l'utente è in grado di sapere se quel dato che è stato violato è importante, sensibile, strategico ecc.

RISPOSTA 3

se la causa della violazione è la carenza tecnologica o organizzativo/procedurale o del singolo individuo e la loro frequenza

RISPOSTA 4

Trasparenza nelle modalità di accesso dei super users (admins) nella infrastruttura CLOUD. In genere, tutti i super user accadono, senza particolari difficoltà o procedure adeguate, a TUTTI i cloud dei clienti. Così facendo si crea un bridge di security dove il router è il super user.

RISPOSTA 5

Riferimenti normativi Policy di gestione degli incidenti report incidenti valutazione della performance dell'erogatore del servizio

RISPOSTA 6

rapporto tra sensibilita' dei dati gestiti e livello di sicurezza offerto via cloud e quindi relativo costo mensile, per esempio: 1)Dati Top Secret livello di sicurezza massimo possibile corrispettivo mensile elevato 2) Dati Sensibili livello di sicurezza molto elevato corrispettivo mensile alto 3) Dati di Interesse livello di sicurezza medio corrispettivo basso

RISPOSTA 7

Sarebbe interessante approfondire il tema dell'impatto della durata della violazione. Ad esempio, l'impatto sulla violazione di una carta di credito ha un valore pari al massimale della carta, ed una durata pari al tempo necessario per sostituirla dopo la segnalazione della violazione. Ma per un furto d'identità? Magari scoperto con mesi o anni di ritardo? L'impatto potrebbe protrarsi per anni, o decine d'anni, in base all'utilizzo che ne è stato fatto.

RISPOSTA 8

E' necessario fornire a priori un mapping del servizio e verificare periodicamente lo status.

RISPOSTA 9

credo che sia essenziale evidenziare che in un contesto di business e di mercato svincolato da limiti territoriali risulta importante avere associazioni di settore con capacità di intervenire in interdizione rispetto gli associati che operano in modo inadeguato/non conforme alle normative applicabili.

