AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

Gli obblighi conseguenti alla violazione di dati personali: il recepimento delle disposizioni comunitarie nell'ordinamento nazionale

di Maurizio Mensi * e Maurizio D'Amico **

SOMMARIO: 1. Premessa – 2. La definizione di "Data Breach" - 3. La nuova disciplina italiana introdotta con il d. lgs. n. 69 del 28 maggio 2012. Le "Linee guida" del Garante per la privacy in materia di "Data Breach Notification" – 3.1. I soggetti tenuti all'obbligo di informativa – 3.2. La comunicazione – 4. Alcune considerazioni.

1. Premessa

Nell'ultimo anno il clamore suscitato da recenti gravi eventi di perdita di dati personali in tutta Europa e nel mondo[1] ha ancor più posto all'attenzione del legislatore comunitario e degli Stati membri la verifica del grado di sicurezza offerto dalla normativa vigente in materia di disciplina dei dati delle persone oggetto di condivisione, trasformazione, archiviazione e trasmissione per via elettronica. Di qui la necessità di definire un quadro regolamentare che garantisca, se necessario, un puntuale ed efficace livello di protezione, anche attraverso la previsione di un sistema di sanzioni adeguato al livello di responsabilità e di professionalità che deve essere richiesto a chi opera in questo delicato settore[2].

* Professore ordinario di Diritto pubblico dell'economia della Scuola Superiore dell'Economia e delle Finanze (SSEF) e di Diritto dell'informazione e della comunicazione presso l'Università "LUISS Guido Carli" di Roma.
** Avvocato specializzato in diritto dell'Unione europea.
Le argomentazioni svolte nel presente articolo riflettono esclusivamente l'opinione degli autori.

[1] Secondo la *Privacy Rights Clearinghouse*, un'organizzazione statunitense *non profit* di consumatori, soltanto negli Stati Uniti tra gennaio 2005 e settembre 2012 sono stati coinvolti in violazioni della sicurezza un totale di circa 563.533.722 singoli *records* contenenti dati personali: v. *https://www.privacyrights.org/data-breach.* Uno dei casi più clamorosi a livello mondiale è avvenuto nel 2011 a danno della *PlayStation Network* della Sony, con la violazione dei dati di almeno cento milioni di utenti.

[2] Il pacchetto di riforma istitutivo di un nuovo quadro giuridico per la protezione dei dati personali nell'Unione europea presentato il 25 gennaio 2012, come delineato nella *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, Al Comitato Economico e Sociale Europeo e al Comitato delle Regioni - "Salvaguardare la privacy in un mondo interconnesso - Un quadro europeo della protezione dei dati per il XXI secolo"* COM (2012) 9 final, si compone di una proposta di regolamento e di una proposta di direttiva.
Si tratta della Proposta di Regolamento del Parlamento europeo e del Consiglio COM (2012) 11 final, "*concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati*

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

La questione è di estrema rilevanza e delicatezza, considerato che lo sviluppo del commercio elettronico (che ha come corollario il deciso nuovo impulso per la *digital economy*, in funzione della promozione della crescita economica e concorrenziale dell'intero comparto industriale europeo) nonché l'evoluzione di nuove applicazioni tecnologiche a medio e lungo termine per la conclusione di accordi contrattuali a distanza, non può assolutamente prescindere dalla fiducia nell'ambiente *on-line* di milioni di cittadini europei. Tale fiducia può essere ottenuta soltanto assicurando un adeguato sistema di garanzie circa la salvaguardia dell'integrità dei dati personali, il cui trattamento informatizzato è prodromico alla fornitura del prodotto, della prestazione o del servizio commerciale richiesti[3].

Per raggiungere tale obiettivo il legislatore comunitario, allo scopo di garantire l'applicazione del quadro normativo già delineato in passato con la direttiva 2002/58/CE[4], aveva in anni recenti emanato, nell'ambito di una complessiva revisione della predetta cd. "direttiva e-privacy", le direttive 2009/136/CE[5] e 2009/140/CE[6], introducendo, a carico dei fornitori delle reti e

---

(regolamento generale sulla protezione dei dati)", e della Proposta di Direttiva del Parlamento europeo e del Consiglio COM (2012) 10 final, "*concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati*". In particolare nelle due proposte normative, rispettivamente negli articoli 31 e 32 e negli articoli 28 e 29 è introdotto l'obbligo generale, e non più settoriale come attualmente è previsto, di notificazione e comunicazione delle violazioni di dati personali, sviluppando la notificazione prevista all'articolo 4, paragrafo 3, della direttiva 2002/58/CE. Tuttavia fra le due proposte esiste una differenza in materia di regolamentazione della comunicazione della violazione dei dati personali all'interessato, dovuta allo specifico settore disciplinato nella direttiva, ossia il trattamento dei dati per ragioni di giustizia e/o di polizia; infatti mentre nella proposta di regolamento se il responsabile del trattamento non ottempera all'obbligo della comunicazione, quest'ultima adempienza può essergli imposta dall'autorità di controllo nazionale in presenza di determinate condizioni, viceversa tale potere coercitivo non è contemplato nella proposta di direttiva: cfr. art. 32, par. 4 della Proposta di Regolamento, *ivi*. e art. 29, par. 4 della Proposta di Direttiva, *ivi*. La presidenza di Cipro del Consiglio dell'Unione europea ha chiarito che intende acquisire un orientamento generale su alcuni articoli del nuovo pacchetto legislativo sulla protezione dei dati già nel mese di dicembre 2012, per riuscire ad adottare tutta la nuova normativa nel 2013 o all'inizio del 2014: cfr. *http://www.cy2012.eu/index.php/en/news-categories/areas/justice-and-home-affairs/feature-step-by-step-towards-data-protection*.

[3] Pertanto il tema della protezione dei dati personali è fondamentale sia per l'Agenda digitale europea (v. *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, Al Comitato Economico e Sociale Europeo e al Comitato delle Regioni – Un'agenda digitale europea* COM (2010) 245 final del 26 agosto 2010) sia a livello più generale, per la "strategia Europa 2020" (v. *Comunicazione della Commissione Europa 2020 – Una strategia per una crescita intelligente, sostenibile e inclusiva* COM (2010) 2020 final del 3 marzo 2010).

[4] Si veda l'art. 4 della direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002,"*relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)*", in *Guce* n. L 201 del 31 luglio 2002, p. 37.

[5] Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009, "*recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori*", in *Guce* n. L 337 del 18 dicembre 2009, p. 11.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

dei servizi di comunicazione elettronica, un sistema europeo di notifica delle violazioni dei dati per il settore delle comunicazioni elettroniche.

Inoltre la decisa propensione delle istituzioni comunitarie ad accelerare la realizzazione del processo di riforma del quadro giuridico in tema di salvaguardia dei dati personali, si è accompagnata alla messa a punto di un'articolata campagna di sensibilizzazione sull'utilità dell'adempimento di specifici obblighi informativi.

In quest'ottica deve essere interpretata la recente intensificazione dell'attività dell'Agenzia europea per la sicurezza delle reti e dell'informazione (*European Network and Information Security Agency* - ENISA), realizzata tramite la pubblicazione di rapporti e di studi, o l'organizzazione di convegni e varie altre iniziative espressamente dedicati a questo argomento: ne costituisce un esempio recente il seminario svoltosi nel gennaio 2011 dedicato alla disciplina della notificazione delle violazioni dei dati in Europa.

Il recepimento delle nuove disposizioni comunitarie, che sarebbe dovuto avvenire entro il 25 maggio 2011[7], non è stato uniforme, nei tempi e nelle modalità, nei vari Stati membri. In particolare l'Italia vi ha provveduto adeguando il testo fondamentale in materia di tutela dei dati personali, ossia il d.lgs. n. 196/2003 (il cd. Codice della privacy)[8], apportandovi modifiche sostanziali attraverso l'adozione dei decreti legislativi n. 69[9], e n. 70[10] del 28 maggio 2012, che hanno introdotto specifici obblighi informativi a carico dei fornitori di servizi di comunicazione elettronica accessibili al pubblico nell'ipotesi di violazione dei dati personali, ossia la cd. *data breach notification*, che costituisce l'oggetto specifico di questo scritto.

---

[6] Direttiva 2009/140/CE del Parlamento europeo e del Consiglio del 25 novembre 2009, *"recante modifica delle direttive 2002/21/CE che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica*", in *Guce* n. L 337 del 18 dicembre 2009, p. 37.

[7] Cfr. art. 4, par. 1 della direttiva 2009/136/CE, *cit. supra* nota 5, e art. 5, par. 1, della direttiva 2009/140/CE, *cit. supra* nota 6.

[8] D.lgs. 30 giugno 2003 n.196 "*Codice in materia di protezione dei dati personali"*, in *Guri* n.174 del 29 luglio 2003 - suppl. ord. n.123. Nel prosieguo del presente articolo, si utilizza il termine "Codice della privacy", abbreviato in cod. privacy.

[9] D.lgs. 28 maggio 2012 n.69 *"Modifiche al decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali in attuazione delle direttive 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, e 2009/140/CE in materia di reti e servizi di comunicazione elettronica e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori"*, in *Guri* n.126 del 31 maggio 2012, p. 22. L'adeguamento al mutato contesto normativo comunitario è stato compiuto dando esecuzione alla delega contenuta nella legge del 15 dicembre 2011 n. 217, *Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee - Legge comunitaria 2010*, in *Guri* n. 1 del 2 gennaio 2012, p. 1, scongiurando per il suo ritardato recepimento l'avvio della relativa procedura di infrazione, di cui erano stati diffidati oltre all'Italia anche altri 19 Stati.

[10] D.lgs. 28 maggio 2012 n. 70 *"Modifiche al decreto legislativo 1° agosto 2003, n. 259, recante codice delle comunicazioni elettroniche in attuazione delle direttive 2009/140/CE, in materia di reti e servizi di comunicazione elettronica, e 2009/136/CE in materia di trattamento dei dati personali e tutela della vita privata"*, in *Guri* n.126 del 31 maggio 2012, p. 29.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

La piena attuazione delle nuove disposizioni è peraltro avvenuta soltanto di recente, con l'emanazione da parte del Garante per la privacy delle "linee guida"[11] contenute nel provvedimento n. 221 del 26 luglio 2012 [12], finalizzate ad indicare i soggetti tenuti all'obbligo della notificazione/comunicazione, le ipotesi in cui sussiste l'obbligo di avvisare i contraenti e le altre persone coinvolte, le misure di sicurezza tecniche e organizzative da attuare per avvertire l'Autorità, i contraenti e le altre persone circa un avvenuto "*data breach*", i tempi e i contenuti della comunicazione.

Peraltro alcune misure prescritte nel provvedimento, a giudizio del Garante, devono essere precedute da una consultazione pubblica avviata mediante la pubblicazione in Gazzetta Ufficiale, diretta in particolare alle società di telecomunicazioni e agli Internet *providers*, con la finalità di acquisire ulteriori riscontri utili per valutare l'adeguatezza e le modalità attuative delle predette prescrizioni: qualsiasi osservazione o commento deve pervenire, anche *on line*, entro tre mesi dalla data della pubblicazione della deliberazione, all'indirizzo del Garante per la privacy.

2. La definizione di *Data Breach*

La cronaca ci offre un variegato repertorio delle attività riconducibili nell'alveo della fattispecie illecita della violazione dei dati personali: l'elenco delle infrazioni annovera le ipotesi più eclatanti, come gli attacchi concertati da parte di *black hats*[13] con l'appoggio della criminalità organizzata o di governi nazionali, o anche semplicemente gli incauti smaltimenti di attrezzature informatiche usate o di supporti di memorizzazione dei dati.

[11] Come confermato da una ricerca condotta dall'ENISA, in realtà sono poche le autorità di controllo che hanno elaborato formali linee guida procedurali, in quanto il sistema delle notifiche non è ancora obbligatorio nella maggior parte dei Paesi.

[12] Deliberazione del Garante per la Protezione dei dati Personali del 26 luglio 2012, n. 221 *"Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali"*, in *Guri* n. 183 del 7 agosto 2012, p. 67. Con l'emanazione di tali linee guida, il Garante ha ottemperato a quanto previsto nell'art. 32-*bis*, comma 6 del Codice della privacy, come modificato dal d. lgs. n. 69/2012, *"Il Garante può emanare, con proprio provvedimento, orientamenti e istruzioni in relazione alle circostanze in cui il fornitore ha l'obbligo di comunicare le violazioni di dati personali, al formato applicabile a tale comunicazione, nonché alle relative modalità di effettuazione, tenuto conto delle eventuali misure tecniche di attuazione adottate dalla Commissione europea ai sensi dell'articolo 4, paragrafo 5, della direttiva 2002/58/CE, come modificata dalla direttiva 2009/136/CE*", nonché in via generale alle disposizioni di cui all'art. 154, comma 1, lett. *c*) cod. privacy.

[13] Il termine indica gli *hackers* malintenzionati o che agendo con intenti criminali, utilizzano le personali elevate capacità di tipo informatico per finalità illecite: l'ipotesi tipica è quella di persone che mantengono segrete le loro conoscenze circa la vulnerabilità di un determinato sistema informatico e gli *exploits* (ossia i codici che permettono l'acquisizione di privilegi o i cd. *denial of service* di determinati computer) che scoprono a proprio vantaggio, non rivelandoli né al pubblico né ai proprietari per consentire loro di apportarvi le necessarie correzioni. Un'efficace definizione di *black hat* è quella di un *hacker* che "*violates computer security for little reason beyond maliciousness or for personal gain*", in R. Moore, *Cybercrime: Investigating High Technology Computer Crime*, 2005, Matthew Bender & Company, p. 258.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

Un'elencazione più analitica può comprendere le seguenti attività: il furto o la perdita di mezzi di comunicazione digitali, (come nastri, dischi rigidi del computer o computer portatili contenenti tali supporti, chiavette USB) su cui sono memorizzate le informazioni in chiaro; la divulgazione intenzionale o meno di informazioni personali in un ambiente *on line* non sicuro, quale è ad esempio Internet, che non è assoggettabile al diretto controllo da parte di singoli individui per quanto concerne la personale *policy* di sicurezza; il trasferimento di tali informazioni a un sistema che non è completamente aperto, ma non è appropriato o formalmente accreditato a livello di regolamentazione della sicurezza, come ad esempio avviene nel caso dell'invio di *e-mail* in chiaro; il trasferimento dei dati verso i sistemi informativi di soggetti potenzialmente ostili, come ad esempio una società concorrente o una nazione straniera, dove potrebbero essere esposti a tecniche di decrittazione più intense; la perdita o anche la fuoriuscita di dati.

Il grado di nocività di una violazione dei dati è particolarmente elevato nell'ipotesi di un evento che menoma l'integrità di un sistema di sicurezza informatico, in occasione del quale i dati sensibili delle persone[14], i segreti commerciali o le proprietà intellettuali (protetti o riservati) di società vengono copiati oppure vengono trasmessi, visualizzati, rubati o utilizzati da soggetti privi dell'autorizzazione ad accedervi.

A tale riguardo è opportuno sottolineare che l'attenzione mediatica su tale argomento è maggiore quando l'evento lesivo concerne i dati delle persone; al contrario, laddove non sussiste un potenziale danno per i singoli individui, si preferisce non divulgare i casi di cd. *corporate data breaches* o di *government data breaches* in quanto la pubblicità intorno a tali eventi può essere più dannosa della perdita dei dati stessi.

Come si può ben rilevare, l'argomento della riservatezza dei dati e delle esigenze di tutela conseguenti al loro accesso da parte di soggetti non autorizzati, costituisce un tema concettualmente e concretamente riferibile sia alle persone fisiche sia alle persone giuridiche.

Tuttavia la direttiva 2002/58/CE, nell'ambito della predisposizione di un sistema di tutela degli abbonati ad un servizio di comunicazione elettronica accessibile al pubblico, pur essendo diretta, ad integrazione della direttiva 95/46/CE, a salvaguardare i diritti fondamentali delle persone fisiche, ed in particolare il loro diritto alla vita privata, oltre ai legittimi interessi delle persone giuridiche, non impone agli Stati membri "*l'obbligo di estendere l'applicazione della direttiva 95/46/CE alla tutela dei legittimi interessi delle persone giuridiche, tutela che è assicurata nel quadro della vigente normativa comunitaria e nazionale*"[15].

Tale limitazione ha come conseguenza che la definizione dell'utente del servizio di comunicazione elettronica accessibile al pubblico sia riferito esclusivamente alla persona fisica che usufruisca di tale servizio per motivi privati o commerciali, senza esservi necessariamente

[14] In questa categoria di dati sono comprese le informazioni di carattere finanziario, come quelle riguardanti i dati delle carte di credito o quelli bancari, o di carattere sanitario, i comportamenti o gli orientamenti di carattere sessuale, o anche quelle che secondo la terminologia anglosassone sono riconducibili alle *Personally Identifiable Informations* (PII), ossia i numeri di previdenza sociale, i numeri di assicurazione, i numeri della carta d'identità.

[15] Cfr. il *considerando* n. 12 della direttiva 2002/58/CE, *cit. supra*, nota 4: il recepimento in Italia con la legge n. 675/1996, con una scelta ribadita anche con il d. lgs. 196/2003, è avvenuto optando per l'estensione della tutela anche alle persone giuridiche.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

abbonata[16].Pertanto in questo ambito la tutela predisposta nell'ipotesi di *data breaches* è applicabile esclusivamente ai dati personali delle persone fisiche, e non anche delle persone giuridiche.

In base alla direttiva 2002/58/CE, per "violazione di dati personali" si intende la *"violazione di sicurezza che comporta accidentalmente o in modo illecito 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 Comunità"*[17]. Quindi il fattore eziologico della "violazione dei dati personali" può consistere in una fattispecie dipendente o non dipendente dalla volontà umana: oltre all'ipotesi di un evento imprevisto come una calamità naturale o un incendio, si può dunque verificare anche nel caso di un'attività umana, posta in essere intenzionalmente o frutto di una semplice disattenzione.

3. La nuova disciplina italiana introdotta con il d. lgs. n. 69 del 28 maggio 2012. Le "Linee guida" del Garante per la privacy in materia di *Data Breach Notification*

Il 1° giugno 2012, nell'ambito del recepimento delle direttive comunitarie di aggiornamento e di integrazione della riforma del quadro regolamentare nel settore delle comunicazioni elettroniche (introdotto per la prima volta con la cd. "direttiva e-privacy" nel 2002[18]), è entrato in vigore il citato

[16] V. art. 2, par. 2, lett. *a*), della direttiva 2002/58/CE, *loc. cit.*

[17] V. art. 2, par. 2, lett. *i*), della direttiva 2002/58/CE, come modificato dall'art. 2, par. 2, lett. *c*) della direttiva 2009/136/CE, *loc. ult. cit.*

[18] Le modifiche apportate dalle direttive 2009/136/CE e 2009/140/CE hanno comportato l'introduzione di nuovi paragrafi all'art. 4: *"3).In caso di violazione di dati personali, il fornitore di servizi di comunicazione elettronica accessibili al pubblico comunica senza indebiti ritardi detta violazione all'autorità nazionale competente. Quando la violazione di dati personali rischia di pregiudicare i dati personali o la vita privata di un abbonato odi altra persona, il fornitore comunica l'avvenuta violazione anche all'abbonato o ad altra persona interessata. Non è richiesta la notifica di una violazione dei dati personali a un abbonato o a una persona interessata se il fornitore ha dimostrato in modo convincente all'autorità competente di aver utilizzato le opportune misure tecnologiche di protezione e che tali misure erano state applicate ai dati interessati dalla violazione della sicurezza. Tali misure tecnologiche di protezione rendono i dati incomprensibili a chiunque non sia autorizzato ad accedervi. Fatto salvo l'obbligo per i fornitori di informare gli abbonati e altri interessati, se il fornitore di servizi non ha provveduto a notificare all'abbonato o all'interessato la violazione dei dati personali, l'autorità nazionale competente, considerate le presumibili ripercussioni negative della violazione, può obbligare il fornitore in questione a farlo. 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. 4) Fatte salve eventuali misure tecniche di attuazione adottate a norma del paragrafo 5, le autorità nazionali competenti possono emanare orientamenti e, ove necessario, stabilire istruzioni relative alle circostanze in cui il fornitore ha l'obbligo di comunicare le violazioni di dati personali, al formato applicabile a tale comunicazione, nonché alle relative modalità di effettuazione. Esse possono altresì verificare se i fornitori hanno adempiuto ai loro obblighi di comunicazione a norma del presente paragrafo e irrogano sanzioni appropriate in caso di omissione. I fornitori tengono un inventario delle violazioni dei dati personali, ivi incluse 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 di*

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

d.lgs. n. 69/2012, che ha innovato in maniera sostanziale il Codice della privacy, introducendo, fra l'altro, la nuova disciplina riguardante la gestione delle violazioni di sicurezza nel settore delle comunicazioni elettroniche accessibili al pubblico.

Si rammenta che l'art. 4, comma 1, lett. *b)*, del Codice della privacy (come modificato dall'art. 40, comma 2, lett. *a)* del d.l. n. 201/2011[19], cd. decreto "Salva Italia", convertito con modificazioni dalla l. 214/2011[20], che, con l'obiettivo di limitare gli oneri amministrativi a carico delle imprese, ha espunto dalla definizione di dato personale qualsiasi informazione concernente le persone giuridiche, gli enti pubblici o le associazioni[21]) definisce il dato personale come "*qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*".

Analogamente la definizione di "interessati", per effetto delle modifiche apportate dall'art. 40, comma 2, lett. *b)* del decreto cd. "Salva Italia", è ora limitato soltanto alle persone fisiche alle quali sono riferiti i dati personali.

Tuttavia l'accezione ristretta di "dato personale", da cui deriva che la disciplina che regola le conseguenze della violazione dei dati deve applicarsi nei soli casi di informazioni riguardanti le persone fisiche, non si concilia con i termini utilizzati negli articoli 32 e 32 *bis* del Codice della privacy, che considerando gli "abbonati" e i "contraenti"[22] sembrano far riemergere la tutela anche per le persone giuridiche.

Riguardo alla sopravvivenza ancora in alcune parti del Codice del riferimento agli abbonati, è opportuno precisare che fra le modifiche apportate dal d.lgs n. 69/2012, l'eliminazione del *nomen* "abbonato" in luogo di "contraente", trova giustificazione nell'assicurarne la riferibilità a qualsiasi

---

verificare il rispetto delle disposizioni di cui al paragrafo 3. Nell'inventario figurano unicamente le informazioni necessarie a tal fine. 5) Per assicurare l'attuazione uniforme delle misure di cui ai paragrafi 2, 3 e 4, dopo aver consultato l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'articolo 29 della direttiva 95/46/CE e il Garante europeo della protezione dei dati, la Commissione può adottare misure tecniche di attuazione riguardanti le circostanze, il formato e le procedure applicabili alle prescrizioni in materia di informazioni e comunicazioni di cui al presente articolo. Nell'adottare tali misure, la Commissione coinvolge tutti i soggetti interessati, in particolare al fine di ottenere informazioni sulle migliori soluzioni tecniche ed economiche disponibili ai fini dell'applicazione del presente articolo. Tali misure, intese a modificare elementi non essenziali della presente direttiva completandola, sono adottate secondo la procedura di regolamentazione con controllo di cui all'articolo 14 bis, paragrafo 2".

[19] Cfr. d.l. 6 dicembre 2011, n. 201 - *"Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici*, in *Guri* n. 284 del 6 dicembre 2011, suppl. ord. n. 251, p.1.

[20] Cfr. l. 22 dicembre 2011, n. 214 – "*Conversione in legge, con modificazioni, del decreto-legge 6 dicembre 2011, n. 201, recante disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici"*, in *Guri* n. 300 del 27 dicembre 2011, suppl. ord. n. 276, p.1.

[21] Tale esclusione comporta un sostanziale ridimensionamento dell'ambito di tutela della riservatezza riferita alle persone giuridiche, per le quali il trattamento dei dati che le riguardano potrà avvenire senza dover chiedere il consenso, come è previsto invece per i dati relativi alle persone fisiche.

[22] Per "contraente" si intende "*qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate":* v. art. 4, comma 2, lett. *f)*, cod. privacy, come modificato dall'art. 1 del d.lgs. n. 69/2012, *cit. supra*, nota 8.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

forma di "rapporto" del consumatore con il *provider* di un servizio di comunicazione elettronica, e sia quindi preferibile abbandonare una nozione un po' obsoleta che, limitandosi al rapporto di abbonamento al servizio, non comprende altre forme oggettivamente più diffuse e che interessano diversi strati ed età dell'utenza (si pensi, ad esempio, all'utilizzo delle carte prepagate).

Su tale questione si era peraltro già espresso il Garante in occasione del parere fornito al Ministro dello Sviluppo Economico e delle infrastrutture e dei trasporti in merito alla proposta di uno schema di decreto legislativo di recepimento della direttiva 2009/136/CE[23]. In particolare, poiché mutando il termine utilizzato, il contenuto della definizione risultava comunque inalterato, il Garante pur ritenendo non necessaria la suddetta modifica, anche in considerazione del fatto che *"sopprimendo il termine "abbonato" se ne perderebbe l'efficacia evocativa, immediatamente associabile, nell'uso comune ormai radicato, allo specifico settore delle comunicazioni (a fronte di un termine, qual è "contraente", molto più ampio e generico)"* l'aveva peraltro accettata, sul presupposto che *"se, come sembra, il nomen della definizione viene modificato nel codice delle comunicazioni elettroniche è opportuno che sia modificato anche nel Codice in materia di protezione dei dati personali che di quella definizione recepisce il contenuto"*[24].

Tuttavia come ha avuto modo di rilevare il Garante nel predetto parere, per eliminare l'incongruenza, foriera di oggettiva confusione, fra la definizione di dato personale, dopo la novella effettuata con l'art. 40 del d.l. n. 201/2011 che ha espunto il riferimento alle persone giuridiche, agli enti e alle associazioni, e la definizione di "contraente" e, laddove viene ancora citato forse per una dimenticanza del legislatore delegato del 2012 (ad esempio nell'art. 32, comma 3), quella di "abbonato" che invece lo riaccolgono, sarebbe stato opportuno integrare la nuova formulazione delle nozioni di "dato personale" e di "interessato", così da farvi *"rientrare, limitatamente al trattamento dei dati nel settore delle comunicazioni elettroniche, rispettivamente, le persone giuridiche, gli enti ed associazioni in quanto "abbonati" ad un servizio di comunicazione elettronica, e i dati relativi a tali soggetti"*[25].

Alla luce del fatto che tali suggerimenti del Garante non sono stati accolti nel d.lgs. n. 69/2012, permane questa discrepanza: da un lato tutte le disposizioni del Codice della privacy riguardanti gli interessati, ovvero il trattamento di dati personali, sono state limitate in via esclusiva alle persone fisiche ed ai trattamenti dei dati personali ad esse relative, dall'altro non è stato modificato l'oggetto della definizione di "abbonato" e di "contraente" nell'ambito della disciplina relativa ai servizi di comunicazione elettronica accessibili al pubblico, che risulterebbe quindi, in base al dato testuale, tuttora applicabile anche alle persone giuridiche.

Peraltro, se si dovesse optare per tale interpretazione, risulterebbe vanificata l'espressa *ratio* dell'introduzione del comma 2 dell'art. 40 del precitato cd. decreto "Salva Italia", ossia "la riduzione degli oneri in materia di privacy" per le imprese.

---

[23] V. Provvedimento del 29 marzo 2012, n. 119 - *Parere del Garante al Ministro dello sviluppo economico e delle infrastrutture e dei trasporti in ordine a uno schema di decreto legislativo recante attuazione della direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009*, reperibile sul sito web *http://www.garanteprivacy.it/garante/doc.jsp?ID=1893400*.

[24] V. Provvedimento del 29 marzo 2012, n. 119, *loc. cit.*

[25] V. Provvedimento del 29 marzo 2012, n. 119, *loc. ult. cit.*

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

In attesa di un'eventuale ulteriore modifica legislativa che rimuova tale incongruità terminologica, non essendo stata accolta nel d.lgs. 69/2012 la proposta fornita dal Garante nel provvedimento n.119/2012 diretta ad integrare le nozioni di "dato personale" e di "interessato" nel modo poc'anzi citato e, a meno di disattendere il precitato obiettivo di semplificazione amministrativa ispiratore della novella del d.l. del 201/2011, si ritiene proponibile l'interpretazione di seguito esposta. In base al combinato disposto delle definizioni di cui all'art. 4, comma 1, lett. *b)*, e comma 2, lett. *f)* cod. privacy, e della disciplina prevista nei successivi artt. 32 e 32 *bis*, è plausibile che ai soli fini della tutela conseguente alla violazione dei dati personali per effetto dell'attività posta in essere dai fornitori di servizi di comunicazione elettronica accessibili al pubblico, gli adempimenti previsti a carico di questi ultimi siano a protezione dei diritti, oltre che degli interessati, soltanto degli abbonati-contraenti persone fisiche[26].

Il Codice della privacy, novellato dall'intervento del legislatore delegato del 28 maggio 2012[27], considera l'attività lesiva dei dati personali come la *"violazione della sicurezza che comporta anche accidentalmente*[28] *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*[29]*"*.

Come nel caso della previsione comunitaria, viene accolta una definizione da un lato piuttosto ampia, comprendente eventi anche non realizzati in maniera intenzionale, dall'altro più limitata, che si applica soltanto ad un settore dei servizi (ossia quello delle comunicazioni

[26] Tale interpretazione restrittiva si conforma, fra l'altro, all'orientamento contenuto nel pacchetto di riforma presentato dalla Commissione europea il 25 gennaio 2012, che preconizzando uno scenario europeo di tutela riguardante i dati delle persone fisiche, considera soltanto la figura dell'"interessato" definito nell'art. 4, par. 1, n. 1 della Proposta di Regolamento, *cit. supra* nota 2 e nell'art. 3, par. 1, n. 1 della Proposta di Direttiva, *ivi*, *"la persona fisica identificata o identificabile, direttamente o indirettamente, con mezzi che il responsabile del trattamento o altra persona fisica o giuridica ragionevolmente può utilizzare, con particolare riferimento a un numero di identificazione, a dati relativi all'ubicazione, a un identificativo on line o a uno o più elementi caratteristici della sua identità genetica, fisica, fisiologica, psichica, economica, culturale o sociale"*. Quando vi siano le condizioni, a tale soggetto, in base all'art. 32, par. 1 della Proposta di Regolamento e art. 29, par. 1 della Proposta di Direttiva deve essere indirizzata la comunicazione dell'avvenuta violazione *"senza ingiustificato ritardo"*. Inoltre a tale riguardo giova rammentare che il *considerando* n. 12 della Proposta di Regolamento precisa espressamente che *"La protezione offerta dal presente regolamento non potrà essere invocata per il trattamento dei dati relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compreso il nome, la forma giuridica e i contatti. Ciò vale anche quando il nome della persona giuridica contiene il nome di una o più persone fisiche"*.

[27] V. art. 4, comma 3, lett. *g-bis)*, cod. privacy, come modificato dall'art. 1 del d.lgs. n. 69/2012, *cit. supra* nota *8*.

[28] Il testo ricalca sostanzialmente il contenuto dell'art. 2, par. 2, lett. *i)*, della direttiva 2002/58/CE, come modificato dall'art. 2, par. 2, lett. *c)* della direttiva 2009/136/CE, *cit. supra*, nota 4.

[29] V. art. 4, comma 2, lett. *e)*, cod. privacy, *cit. supra* nota 8, in base al quale tali servizi sono quelli consistenti *"esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002)*". Per rete di comunicazione elettronica si intende quella *"utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti")*, v. art. 4, comma 2, lett. *d)*, cod. privacy, *ivi*.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

elettroniche accessibili al pubblico) e per una cerchia soggettiva specifica (soltanto i fornitori dei servizi, ad esempio, quelli telefonici o di accesso ad Internet)[30].

Ottemperando al principio comunitario di salvaguardia della sicurezza[31] recepito dall'art. 31[32], i fornitori di servizi di comunicazione elettronica accessibili al pubblico sono tenuti ad adottare, anche attraverso altri soggetti ai quali ne sia affidata l'erogazione (ossia ad esempio per i servizi affidati in *outsourcing*), misure tecniche ed organizzative adeguate al rischio esistente[33]. Tali misure debbono essere altresì idonee a salvaguardare la tutela dei dati archiviati o trasmessi rispetto a determinati eventi[34], anche di natura soltanto accidentale, per la protezione della sicurezza dei loro servizi e per adempiere agli obblighi prescritti dall'articolo 32-*bis*.

Inoltre i soggetti operanti sulle reti di comunicazione elettronica garantiscono che i dati personali siano accessibili soltanto al personale autorizzato per fini legalmente autorizzati[35].

Viene altresì introdotto un ulteriore obbligo di carattere generale: quello di attuare una vera e propria politica di sicurezza: ossia viene imposto alle società che trattano dati personali di adottare un approccio sistematico e strutturale nella gestione della sicurezza in questo delicato settore.

Nell'ipotesi in cui la salvaguardia della sicurezza dei servizi o dei dati personali comporti anche l'individuazione di misure concernenti le reti di comunicazione, è prevista una particolare sinergia operativa per l'adozione delle misure, che dovranno essere il frutto di un'adozione

[30] Tale limitazione settoriale comporta che non sarà applicabile la disciplina in oggetto se la banca dati potenzialmente soggetta al rischio di intrusione informatica, e quindi di violazione dei dati, non è riferibile direttamente all'attività del servizio offerto dal *provider*, bensì ad altre attività aziendali, come ad esempio il settore della gestione delle risorse umane o quello contabile.

[31] Cfr. art. 4, par. 1 della direttiva 2002/58/CE, *cit. supra*, nota 4. "*Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve prendere appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi, se necessario congiuntamente con il fornitore della rete pubblica di comunicazione per quanto riguarda la sicurezza della rete. Tenuto conto delle attuali conoscenze in materia e dei loro costi di realizzazione, dette misure assicurano un livello di sicurezza adeguato al rischio esistente*".

[32] A questo dovere di carattere generale è connesso l'obbligo di adottare misure minime di sicurezza ai sensi dell'art. 33 cod. privacy, che in difetto espongono i titolari del trattamento di dati alle conseguenze di carattere penale previste nel successivo art. 169. Il novero delle predette misure dovrebbe consistere in: soluzioni tecniche idonee ad impedire la disponibilità dei dati per ulteriori elaborazioni da parte di sistemi informativi altrui al termine delle attività realizzate e nelle quali tali dati sono coinvolti, per esempio mediante il ricorso a metodologie crittografiche o di anonimizzazione; tecnologie informatiche capaci di garantire la possibilità del monitoraggio, da parte di ciascun incaricato del trattamento, delle attività realizzate sui dati personali; misure di sicurezza specifiche per i dispositivi informatici portatili.

[33] V. art. 32, comma 1, cod. privacy, *loc. cit.* Ciò comporta che i *providers* debbano preliminarmente effettuare una disamina delle diverse tipologie di informazioni personali da essi trattati, associarli a determinate caratteristiche di rischio potenziale, secondo specifici gradi di pericolosità crescente e, successivamente, scegliere le misure di sicurezza più adeguate alle predette risultanze.

[34]Sono i seguenti: a) distruzione anche accidentale; b) perdita o alterazione anche accidentale; c) archiviazione; d) trattamento; e) accesso o divulgazione non autorizzati o illeciti (v. art. 32, comma 1-*ter*, *loc. ult. cit.).*

[35] V. art. 32, comma 1-*bis*, *cit. supra* nota 8.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

congiunta da parte dei fornitori del servizio di comunicazione elettronica accessibile al pubblico e dei fornitori della rete pubblica di comunicazioni[36].

3.1. I soggetti tenuti all'obbligo di informativa

Nel caso di violazione dei dati personali vengono stabiliti specifici obblighi di comunicazione per i fornitori di servizi di comunicazione elettronica accessibili al pubblico, compreso il caso di affidamento dell'erogazione di tali servizi a diversi soggetti, come ad esempio avviene nell'ipotesi dei servizi affidati in *outsourcing* (in base al nuovo articolo 32-*bis* intitolato "*Adempimenti conseguenti ad una violazione di dati personali*").

Una più precisa individuazione dei soggetti obbligati, come indicato nelle "linee guida", è contenuta nel provvedimento del Garante del 17 gennaio 2008[37]. Nel documento è indicato che per "*fornitori di servizi di comunicazione elettronica accessibili al pubblico*", s'intendono 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)"*.

Tali obblighi non operano invece per le reti aziendali[38], gli *Internet points*[39], i motori di ricerca[40], i siti internet che diffondono contenuti o cd. "*content provider*"[41].

---

[36] Nell'ipotesi in cui non sia raggiunta una scelta condivisa, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente.
Bisogna ricordare che a carico dei fornitori viene individuato lo specifico obbligo dell'informativa concernente l'esistenza di *"un particolare rischio di violazione della sicurezza della rete":* v. art. 32, comma 3, *loc. cit.* In questa informativa devono essere precisati, se la fattispecie di rischio è al di fuori dell'ambito di applicazione delle precitate misure, tutti i possibili rimedi e i relativi costi presumibili: in tal caso destinatario della comunicazione oltre al Garante, agli abbonati e, se possibile, agli utenti, è anche l'Autorità per le garanzie nelle comunicazioni.

[37] Provvedimento 17 gennaio 2008 "*Conservazione dei dati di traffico: misure e accorgimenti a tutela dell'interessato in attuazione dell'articolo 132 del decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali*", in *Guri* n. 30 del 5 febbraio 2008, p. 62, come modificato e integrato dal Provvedimento 24 luglio 2008 "*Modifica al provvedimento del 17 gennaio 2008 sulla conservazione dei dati di traffico - Misure e accorgimenti a tutela dell'interessato in attuazione dell'articolo 132 del decreto legislativo 30 giugno 2003, n. 196, recante: «Codice in materia di protezione dei dati personali»*", in *Guri* n. 189 del 13 agosto 2008, p. 32.

[38] I "*soggetti che offrono direttamente servizi di comunicazione elettronica a gruppi delimitati di persone (come, a titolo esemplificativo, i soggetti pubblici o privati che consentono soltanto a propri dipendenti e collaboratori di effettuare comunicazioni telefoniche o telematiche). Tali servizi, pur rientrando nella definizione generale di "servizi di comunicazione elettronica", non possono essere infatti considerati come "accessibili al pubblico". Qualora la comunicazione sia instradata verso un utente che si trovi al di fuori della c.d. "rete privata", i dati di traffico generati da tale comunicazione sono invece oggetto di conservazione (ad es., da parte del fornitore di cui si avvale il destinatario della comunicazione, qualora si tratti di un messaggio di posta elettronica; cfr. documento di lavoro "Tutela della vita privata su Internet – Un approccio integrato dell'EU alla protezione dei dati on-line", adottato dal Gruppo di lavoro per la tutela dei dati personali il 21 novembre 2000)*", in Provvedimento 17 gennaio 2008, *cit. supra* nota 37.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

Nell'ipotesi in cui i servizi siano affidati dai *providers* ad altri soggetti, esterni alla loro organizzazione aziendale, si applica il comma 8 dell'art. 32-bis, in base al quale i soggetti affidatari devono comunicare *"senza indebito ritardo al fornitore tutti gli eventi e le informazioni necessarie a consentire a quest'ultimo di effettuare gli adempimenti"* previsti, quando si verifica una violazione di dati personali.

I soggetti destinatari di tale obbligo sono ad esempio i cd. operatori virtuali di rete mobile (*Mobile Virtual Network Operator*, MVNO), ossia le società che forniscono servizi di telecomunicazione mobile al pubblico, pur non possedendo alcuna licenza per il relativo spettro radio né le infrastrutture necessarie per fornire questi servizi, e che si avvalgono a tale scopo di una parte dell'infrastruttura di uno o più operatori mobili reali (*Mobile Network Operator* - MNO) sulla base di un accordo, commerciale o regolamentato[42].

Poiché gli operatori mobili virtuali dispongono di numerazioni o archi di numerazione telefonica (*Mobile Subscriber ISDN Number* - MSISDN) propri e, di conseguenza, di proprie SIM *card* (*Subscriber Identification Module*), che emettono e convalidano[43], essi utilizzano il proprio apparato strutturale di commutazione di rete mobile, le proprie funzioni di trasporto, la propria base di dati di registrazione dei loro utenti di telefonia mobile (HLR, *Home Location Register*), nonché la propria attività di gestione dei clienti (aree commercializzazione, fatturazione, assistenza). Pertanto pur essendo il servizio erogato, dal punto di vista operativo, dagli MNO, sono soltanto gli operatori virtuali che hanno un rapporto diretto con i clienti, con i quali viene stipulato il contratto e che quindi, a differenza degli operatori mobili reali, conoscono la loro identità.

---

[39] *Ivi,* in particolare "*i titolari e i gestori di esercizi pubblici o di circoli privati di qualsiasi specie che si limitino a porre a disposizione del pubblico, di clienti o soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, ovvero punti di accesso a Internet utilizzando tecnologia senza fili, esclusi i telefoni pubblici a pagamento abilitati esclusivamente alla telefonia vocale*".

[40] Ciò in quanto il trattamento delle informazioni relative al traffico telematico, che viene utilizzato per fare una tracciatura delle operazioni realizzate dall'utente in rete, è equiparabile ai "contenuti".

[41] "Essi non sono, infatti, fornitori di un "servizio di comunicazione elettronica" come definito dall'art. 4, comma 2, lett. *e*) del Codice. Tale norma, infatti, nel rinviare, per i casi di esclusione, all'art. 2, lett. *c*) della 2002/21/CE cit., esclude essa stessa i "*servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica* […]", *loc. ult. cit.*

[42] Cfr. le definizioni contenute nella Delibera dell'Autorità per le garanzie nelle comunicazioni 1° agosto 2000 - *Condizioni regolamentari relative all'ingresso di nuovi operatori nel mercato dei sistemi radiomobili*, n. 544/00/CONS, in *Guri* n. 183 del 7 agosto 2000, p. 61.

[43] Per far ciò l'MVNO si deve preliminarmente dotare di un proprio codice di rete mobile (*Mobile Network Code* - MNC), attraverso il quale possono essere generati gli IMSI (*International Mobile Subscriber Identity*) delle SIM *card*. In tale ipotesi l'operatore si definisce *Full Mobile Virtual Network Operator* (*Full* MVNO). Se invece non è abilitato all'utilizzo di proprie SIM *card*, demandandone l'emissione all'operatore mobile reale, il soggetto si definisce *Enhanced Service Provider* (ESP MVNO) e dispone soltanto di proprie infrastrutture per fornire servizi a valore aggiunto (*Value Added Services* – VAS, ossia tutti i servizi non qualificati come servizi di base, ovvero le chiamate di voce standard e le trasmissioni tramite fax, e che consistono ad esempio nelle tecnologie sms, mms e gprs) e quelle per la commercializzazione dei prodotti. Infine quando le funzioni svolte riguardano esclusivamente i settori del *marketing*, del *branding* e della vendita, mentre tutti gli altri processi sono gestiti dall'MNO, l'operatore è definito *Service Provider* MVNO (SP MVNO).

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

In base a tali considerazioni si giustifica l'imposizione di questa specifica incombenza, in funzione complementare all'adempimento principale dovuto dai fornitori nei confronti del Garante, ed eventualmente, dei contraenti e delle altre persone interessate. Pertanto nelle "linee guida" è specificato che il termine per l'adempimento della comunicazione al fornitore è fissato in ventiquattro ore decorrenti dall'avvenuta conoscenza della violazione.

Un'altra categoria di operatori riguardati dal predetto comma 8 è definita dai fornitori che affidano in *outsourcing* l'erogazione dei servizi, anche soltanto in maniera parziale, a soggetti esterni alla loro organizzazione aziendale per ottimizzare i relativi costi.

3.2. La comunicazione

Il principale soggetto cui deve essere comunicato l'evento intrusivo è il Garante per la privacy al quale, in base al contenuto delle "linee guida", deve essere inoltrata una sommaria informativa entro ventiquattro ore dalla scoperta dell'evento[44], ai fini di una prima informazione iniziale che consenta comunque all'Autorità di controllo di determinare il grado di violazione[45].

Nei tre giorni successivi le società telefoniche o gli *Internet providers* hanno l'obbligo di informare dettagliatamente, secondo le modalità ritenute più adatte, anche i contraenti o i terzi soggetti coinvolti[46] (nell'ipotesi di violazioni più gravi, ossia quando la stessa violazione rischia di procurare loro un pregiudizio), nonché il Garante, nel qual caso l'informativa verte, fra l'altro, sulla descrizione dettagliata dei rimedi proposti o adottati e delle misure di prevenzione messe in atto[47].

Non è difficile comprendere quale rilevanza abbia l'ottemperanza da parte dei fornitori a tale obbligo nei tempi previsti, in quanto il fattore temporale è cruciale per consentire ai titolari dei dati

[44] La tassatività del termine non è riscontrabile nella direttiva 2009/136/CE che, invece, prescrive l'effettuazione dell'adempimento, genericamente, *"senza indebiti ritardi"*: v. art. 2, par. 4, lett. *c*) della direttiva 2009/136/CE, *cit. supra*, nota 5. Invece la quasi perentorietà del rispetto del termine delle ventiquattro ore è presente sia nella proposta di regolamento (art. 31, par. 1), sia nella proposta di direttiva (art. 28, par. 1) del 25 gennaio 2012, *cit. supra*, nota 2. Tuttavia, a tale riguardo, è opportuno evidenziare che il Garante europeo per la protezione dei dati (GEPD) nel parere del 7 marzo 2012 sul pacchetto di riforma della protezione dei dati (in *Guce* n. C 192 del 30 giugno 2012, p. 7) presentato dalla Commissione Europea, ha chiesto di prolungare il termine previsto nella proposta di regolamento da ventiquattro a settantadue ore.

[45] Nella comunicazione devono essere tassativamente elencati i seguenti elementi: a) generalità del fornitore; b) breve descrizione della violazione; c) data anche presunta della violazione e del momento della sua scoperta; d) luogo in cui si è verificata la violazione, anche nell'ipotesi in cui essa sia avvenuta successivamente allo smarrimento di dispositivi o di supporti portatili; e) natura e contenuto dei dati, anche soltanto presumibilmente coinvolti; f) sintetica descrizione dei sistemi di elaborazione o di memorizzazione utilizzati per il trattamento dei dati coinvolti, con indicazione della loro ubicazione.

[46] Inoltre come ulteriore incombenza connessa, in base al nuovo articolo 132-*bis* cod. privacy, introdotto dal d. lgs. n. 69/2012, i fornitori sono anche obbligati all'istituzione di apposite e specifiche procedure interne per ottemperare alle richieste di accesso a propri dati personali trasmesse dai contraenti o da altre persone, dovendo altresì fornire al Garante, se lo richiede, le informazioni su tali procedure, sul numero di richieste ricevute, sui motivi legali addotti e sulle risposte date.

[47] V. art. 32-*bis*, comma 5, *cit. supra*, nota 8. A tale riguardo per agevolare questo adempimento il Garante ha elaborato un modello di comunicazione che è disponibile *on line* sul sito *www.garanteprivacy.it*.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

di poter in qualche modo tutelarsi e tentare di limitare gli effetti pregiudizievoli derivanti da tali infrazioni.

La scelta dello strumento di comunicazione dipende anche dal numero dei soggetti che devono essere avvertiti: quindi nell'ipotesi di una pluralità di destinatari sarà più opportuno l'utilizzo di forme di comunicazione *erga omnes* o ad effetto diffuso, come ad esempio la pubblicazione di comunicati su testate giornalistiche generaliste o di settore, anche *on line*, o su emittenti radiofoniche, anche locali, o avvalendosi delle varie forme di interrelazione presenti su Internet, come *blog*, *forum*, *social network*, ecc.

Per la valutazione della gravità dell'evento, da cui consegue la necessità dell'obbligo di comunicazione, occorre conformarsi ai criteri prestabiliti nelle "linee guida", secondo cui rileva la qualità dei dati, che possono essere quelli definibili come sensibili (finanziari, sanitari, giudiziari), la loro "attualità" (le informazioni più recenti sono in generale più appetibili per gli *hackers*), il grado di pregiudizio che la perdita o la distruzione dei dati può comportare (furto o usurpazione di identità, danno fisico, umiliazione grave o danno alla reputazione[48]), la quantità dei dati coinvolti.

L'obbligo dell'informativa non vige se il fornitore dimostra al Garante di aver utilizzato misure tecnologiche di protezione (per esempio consistenti in dispositivi crittografici, basati su algoritmi standardizzati o su funzioni di *hashing*, e in tecniche di anonimizzazione) che rendono i dati non intelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate ai dati oggetto della violazione[49].

I *provider*s sono tenuti a predisporre un inventario, che deve essere regolarmente aggiornato, delle violazioni subite, delle circostanze nelle quali esse sono avvenute, delle loro conseguenze e dei provvedimenti che sono stati adottati per rimediarvi, esclusivamente per consentire al Garante la verifica del rispetto delle disposizioni normative applicabili[50]. A tale ultimo riguardo nell'inventario dovrà essere riportato soltanto il complesso delle informazioni necessarie all'effettuazione di questo tipo di controllo[51].

La conseguenza della mancata comunicazione al Garante della violazione dei dati personali o per l'ipotesi di provvedimento adottato in ritardo consiste in una sanzione amministrativa compresa fra venticinquemila e centocinquantamila euro; analogamente per l'omessa o mancata

[48] Cfr. il *considerando* n. 61 della direttiva 2009/136/CE, *cit.* supra, nota 5.

[49] V. art. 32-*bis*, comma 3, cod. privacy, *cit. supra*, nota 8. La precedente ipotesi di esonero non ha valenza assoluta e deve essere interpretata in connessione con il successivo comma 4, in quanto, come ricordato dal Garante, l'utilizzo di sistemi astrattamente idonei a conferire ai dati personali la qualità dell'intelligibilità a soggetti non autorizzati, riduce ma non elimina totalmente il rischio reale di una loro possibile violazione e, quindi, del possibile avvio della procedura di comunicazione coattiva su disposizione dell'Autorità di controllo: tale ultima eventualità dipenderà anche dall'esito del giudizio sull'operato complessivo del fornitore in materia di salvaguardia della sicurezza e dalle caratteristiche della fattispecie violativa concretamente descritta, in relazione a quanto previsto nel precitato comma 5. Tuttavia, secondo il Garante, i fornitori sono comunque sempre obbligati a comunicare repentinamente ai contraenti le violazioni concernenti il nome utente e/o la password (prescindendo che quest'ultima sia criptata o oggetto di *hashing*) o le chiavi di cifratura adoperate dai contraenti stessi.

[50] V. art. 32-*bis*, comma 7, *loc. cit.*

[51] Per salvaguardare l'integrità del contenuto dell'inventario, i fornitori sono tenuti ad utilizzare misure adeguate ad assicurare che le informazioni riportate siano inviolabili e non modificabili.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

comunicazione ai contraenti e alle altre persone interessate la sanzione è compresa fra centocinquanta e mille euro per ciascun contraente o altra persona nei cui confronti viene omessa o ritardata la comunicazione[52].

Ai sensi dell'art. 162-*ter*, comma 5, le medesime sanzioni si applicano anche nei confronti dei soggetti affidatari dell'erogazione dei servizi, responsabili per l'omessa comunicazione senza ritardo ai fornitori di tutte le informazioni necessarie agli stessi per gli adempimenti di cui all'articolo 32-*bis*.

Infine l'omessa tenuta dell'inventario aggiornato è punita con la sanzione da 20 mila a 120 mila euro[53].

4. Alcune considerazioni

Alcune considerazioni a commento dell'impianto regolamentare entrato in vigore il 1° giugno 2012 non possono non prendere le mosse dalla constatazione che il cammino da percorrere, per rendere effettiva la creazione di un quadro normativo armonizzato nell'area comunitaria in materia di protezione dei dati personali esposti a fattispecie violative, è ancora piuttosto lungo e dall'esito incerto.

L'obiettivo è quello di creare un quadro giuridico condiviso da coloro ai quali è destinato e al tempo stesso corrispondente alle aspettative di tutela dei diritti fondamentali[54] di milioni di

[52] In tale ipotesi non si applica al fornitore il beneficio del cumulo giuridico previsto dall'art. 8 della legge 24 novembre 1981, n. 689. Tuttavia le modifiche introdotte dal d.lgs. n. 69/2012 prevedono una mitigazione della valenza della sanzione consistente nel fatto che essa non può essere applicata in misura superiore al cinque per cento del volume d'affari realizzato dal fornitore nell'ultimo esercizio chiuso precedentemente alla notificazione della contestazione della violazione amministrativa: peraltro tale previsione non pregiudica l'applicazione della speciale accentuazione dell'entità della sanzione per renderla più efficace, consistente nel suo aumento fino al quadruplo, in relazione alle condizioni economiche del contravventore, ai sensi dell'art. 164-*bis*, comma 4, *cit. supra* nota 8.

[53] Da ultimo si ricorda l'esistenza della pena detentiva di cui all'art. 168 cod. privacy consistente, salvo che il fatto costituisca un più grave reato, nella reclusione da sei mesi a tre anni prevista nei confronti sia dei fornitori che dichiarino o attestino falsamente notizie o circostanze, o producano atti o documenti falsi in occasione della comunicazione al Garante conseguente alla violazione di dati personali, sia dei soggetti affidatari dell'erogazione del servizio, che effettuino false comunicazioni ai fornitori.

[54] Giova ricordare la rilevanza cui è assurta in ambito comunitario la materia della tutela della riservatezza delle persone sancita con l'introduzione dell'articolo 8 in tema di protezione dei dati personali nella Carta dei diritti fondamentali dell'Unione europea, e dell'articolo 16, paragrafo 1 nel Trattato sul funzionamento dell'Unione europea (nuova denominazione del Trattato istitutivo CE): v. rispettivamente *Carta dei diritti fondamentali dell'Unione europea*, proclamata il 7 dicembre 2000, in *Guce* n. C 364 del 18 dicembre 2000, p. 1, nonché la versione adattata che ha sostituito il testo del 2000, a decorrere dall'entrata in vigore del Trattato di Lisbona, in *Guce* n. C 83 del 30 marzo 2010, p. 389, e *Trattato di Roma del 25 marzo 1957. Trattato che istituisce la Comunità Economica Europea*, sottoscritto a Roma il 25 marzo 1957, ratificato con l. 14 ottobre 1957, n. 1203, in *Guri* Serie Generale n. 317 del 23 dicembre 1957, suppl. ord. Dopo l'emanazione del Trattato di Lisbona (*Trattato di Lisbona che modifica il trattato sull'Unione europea e il trattato che istituisce la Comunità europea*, firmato a Lisbona il 13 dicembre 2007, in *Gu-Ue* n. C 306 del 17 dicembre 2007, p. 1) la nuova denominazione è la seguente: *Trattato 25 marzo 1957. Trattato sul funzionamento*

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

persone oltre che rispettoso delle esigenze delle imprese interessate. Tuttavia, a giudicare dalle prime reazioni che le nuove norme hanno suscitato è lecito nutrire qualche dubbio al riguardo.

La previsione comunitaria è stata trasposta nell'ordinamento nazionale con circa un anno di ritardo rispetto alla data prevista del 25 maggio 2011, in analogia peraltro con quanto avvenuto in altri Paesi membri.

Il mondo imprenditoriale ha accolto con fastidio l'adempimento della notificazione e della comunicazione, unitamente al complesso degli oneri ad essi collegati, percepiti come un inutile e dispendioso appesantimento procedurale.

In realtà l'impianto delineato negli artt. 32 e 32-*bis* del Codice della privacy è volto a consentire alle imprese di configurare la propria struttura aziendale (sia pur soltanto per il settore delle comunicazioni elettroniche accessibili al pubblico) come "*data protection oriented*", così da rendere l'incombenza della notificazione e dell'eventuale comunicazione non come un mero adempimento formale, bensì come uno strumento per una più efficace tutela della sicurezza propria e dei clienti, doverosa peraltro per chi si trova a gestire materiale documentale delicato, quali sono appunto le informazioni personali.

L'ENISA, nelle sue Raccomandazioni dell'aprile 2012[55], ha precisato che è richiesta sistematicità e professionalità nella gestione del rischio e delle eventuali violazioni di dati personali: viene sollecitata quindi la predisposizione di un idoneo piano in cui siano individuate misure tecniche e organizzative di livello commisurato al tipo di minaccia, in grado di garantire risposte tempestive, efficaci e adeguate all'entità della violazione.

Si pone pertanto il problema di valutare le modalità attuative ottimali per la tutela reale dei titolari dei dati personali con il minor dispendio possibile in termini organizzativi e finanziari per le società onerate[56].

Si ritiene per esempio che un approccio basato sull'esatta analisi del rischio e sulla corretta valutazione dei livelli di rischio in rapporto alle varie tipologie di infrazioni sia tale da ridurre notevolmente il numero delle notifiche ai casi in cui queste siano effettivamente necessarie. Ciò consente di evitare adempimenti sproporzionati rispetto a violazioni potenzialmente non gravi e il conseguente aumento dei relativi costi, così da non compromettere la competitività delle imprese del settore.

---

dell'Unione Europea, sottoscritto a Roma il 25 marzo 1957, ratificato con l. 14 ottobre 1957, n. 1203, in *Guri* Serie Generale n. 317 del 23 dicembre 1957, suppl. ord.

[55] Disponibile al seguente indirizzo: *http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech.*

[56] Ad esempio secondo uno studio della Commissione Europea si stima che circa 3.000 notifiche delle violazioni dei dati sono effettuate nell'area UE nel settore delle telecomunicazioni, con un costo pari a circa 20.000 euro per ciascuna di esse (sulla base di 319 violazioni di protezione dei dati segnalati all'Autorità di controllo inglese sui dati personali nel 2008/2009 ed estrapolati per l'Unione Europea).
Se la notifica venisse estesa a tutti i settori, si stima che si potrebbero avere circa 1.000 notifiche in più. Il costo totale addizionale sarebbe quindi valutabile nell'ordine di circa 20 milioni di euro all'anno: *http://ec.europa.eu/justice/dataprotection/document/review2012/sec_2012_72_annexes_en.pdf.*

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

Altresì è opportuno sottolineare che una corretta gestione dei costi può dipendere anche da un'appropriata scelta dei mezzi di comunicazione relativi all'avvenuta infrazione, che spesso può dipendere dalla qualità delle informazioni di contatto a disposizione del titolare del trattamento.

Se una violazione necessita della comunicazione verso una pluralità di persone, potrebbe accadere che le informazioni di contatto risultino obsolete o errate, con la non peregrina eventualità che l'informativa possa essere effettuata ad un indirizzo erroneo o ad una persona sbagliata, e con la paradossale conseguenza che sia proprio il contenuto stesso della comunicazione a divulgare dati personali a soggetti non autorizzati ad accedervi.

Come è stato evidenziato, la nuova disciplina concernente gli obblighi di notificazione al Garante e, in casi determinati, di comunicazione ai contraenti e alle altre persone interessate non si applica alla totalità dei titolari dei trattamenti, ossia dei soggetti, pubblici o privati, che detengono e trattano dati personali in funzione della propria attività.

L'obbligo del "*data breach notification*", attualmente circoscritto dal legislatore italiano a carico soltanto di alcune categorie di soggetti, si differenzia da soluzioni adottate da altri Stati membri che invece si caratterizzano per l'estensione di tale incombenza ad una platea più ampia di soggetti,[57] come avviene ad esempio in Germania, Austria, Regno Unito e Irlanda.

Tuttavia il Garante per la privacy ha adottato un approccio più ampio, in linea con quanto previsto nei Paesi europei poc'anzi citati, come avvenuto con il provvedimento del 12 maggio 2011[58], con cui è stato prescritto alle banche, quale misura ritenuta opportuna, di comunicare tempestivamente ed in maniera analitica all'Autorità di controllo, "*i casi in cui risultino accertate violazioni, accidentali o illecite, nella protezione dei dati personali, purché di particolare rilevanza per la qualità o la quantità di dati coinvolti e/o il numero di clienti interessati, dalle quali derivino la distruzione, la perdita, la modifica, la rivelazione non autorizzata dei dati della clientela*".

Merita di essere ricordato che il "pacchetto" di proposta di riforma della disciplina comunitaria nel settore della protezione dei dati personali, presentato dalla Commissione europea il 25 gennaio 2012[59], contempla l'obbligo generale per tutti i responsabili del trattamento di notificare senza indugio le violazioni di informazioni personali alle autorità di protezione dei dati, se possibile entro ventiquattro ore, e agli interessati "*senza ingiustificato ritardo*".

L'estensione generalizzata di tale adempimento accoglie, fra l'altro, un'esigenza già evidenziata dal legislatore comunitario nel *considerando* n. 59, della direttiva 2009/136/CE: "*L'interesse degli utenti ad essere informati non si limita ovviamente al settore delle comunicazioni elettroniche e, conseguentemente, l'introduzione a livello comunitario di prescrizioni esplicite e obbligatorie relative alla comunicazione delle violazioni dovrebbe ricevere carattere prioritario. In attesa di condurre una revisione di tutta la legislazione comunitaria pertinente, la Commissione, in*

[57] Tale orientamento è conforme alla posizione espressa dal Gruppo dei Garanti europei (c.d. "Gruppo Art. 29") nel *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments* (WP 184), adottato il 5 aprile 2011.

[58] Deliberazione del Garante per la Protezione dei Dati Personali del 12 maggio 2011 – "*Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie*", in *Guri* n. 127 del 3 giugno 2011, p. 70.

[59] *Cit. supra* nota 2.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

consultazione con il Garante europeo della protezione dei dati, dovrebbe adottare senza indugio le misure adeguate a incoraggiare l'applicazione dei principi racchiusi nelle norme relative alla comunicazione delle violazioni dei dati di cui alla direttiva 2002/58/CE (direttiva relativa alla vita privata e alle comunicazioni elettroniche), indipendentemente dal settore o dal tipo di dati interessati".

Il consolidamento del quadro regolamentare basato sull'obbligo della notificazione/comunicazione è peraltro tale da comportare costi significativi a carico delle imprese (derivanti dalle spese per l'invio delle comunicazioni o quelle derivanti da possibili azioni legali conseguenti a richieste di risarcimento dei danni e/o *class action* intentate individualmente o per gruppi, eventuali sanzioni amministrative pecuniarie, perdite economiche in conseguenza della diminuita fiducia dei clienti). Questo potrà avere come effetto la sottoscrizione da parte delle imprese di polizze volte a limitare tali rischi finanziari (così da rimanere competitive rispetto ai concorrenti non gravati da tali oneri) con compagnie assicuratrici specializzate nella copertura di tali fattispecie. Di qui il probabile sviluppo del mercato europeo delle assicurazioni informatiche o "*cyber insurance*"[60], oggi ancora di scarse dimensioni in Europa.

In ultima analisi merita di essere sottolineato come gli oneri informativi costituiscano un elemento essenziale per assicurare concreta trasparenza e conoscibilità degli eventi intrusivi verificatisi. Dalla loro corretta attuazione dipende, in larga parte, la disponibilità di comunicazioni elettroniche sicure ed affidabili.

Infatti se è vero che esempi eclatanti di violazioni ricevono una copertura mediatica sufficientemente diffusa, si rileva tuttavia che per ragioni derivanti dalla tutela della sicurezza o da esigenze di ordine pubblico molte altre incursioni (se e quando vengono individuate) non sono rese note, risultando confinate ad una ristretta cerchia di "addetti ai lavori" (esperti di sicurezza informatica, riviste specializzate, servizi di sicurezza[61], ecc.)[62].

---

[60] Nel mese di dicembre 2011, la compagnia assicurativa statunitense *Chubb* ha lanciato un nuovo prodotto di *cyber insurance*, nel Regno Unito, in Irlanda e in Europa che tutela i rischi connessi ai dati sensibili, in particolare quelli finanziari e sanitari. Sull'argomento si veda il recente rapporto dell'ENISA pubblicato nel mese di giugno 2012, intitolato "*Incentives and barriers of the cyber insurance market in Europe*".

[61] Per un esempio extra UE, si veda il disegno di legge presentato negli Stati Uniti nel mese di giugno 2012, intitolato *"Data Security and Breach Notification Act of 2012"* che, nell'ipotesi in cui la violazione dei dati riguardi più di diecimila persone, prevede l'obbligo della notifica nel più breve termine possibile anche ai servizi segreti o al *Federal Bureau of Investigation* (FBI).

[62] A tale riguardo sono emblematici tre avvenimenti, che sono citati anche nel recente rapporto dell'ENISA intitolato *Cyber Incident Reporting in the EU - An overview of security articles in EU legislation* pubblicato nel mese di agosto 2012. Nel mese di aprile 2010, un *provider* cinese di telecomunicazioni a partecipazione statale, ha dirottato per circa venti minuti il 15% del traffico Internet mondiale attraverso *server* cinesi: la tracciatura del traffico di alcuni grandi siti di commercio elettronico, come quello della versione tedesca di *amazon* e quello della società *Dell*, nonché di domini .mil e .gov. Il risultato è stato che le comunicazioni Internet di milioni di utenti potrebbero essere state esposte ad intercettazioni.
Durante l'estate 2011, un'autorità di certificazione olandese ha subito una violazione della sicurezza che ha consentito agli aggressori di generare falsi certificati digitali relativi a chiavi crittografiche pubbliche (*public key infrastructure* - PKI), i quali sono stati utilizzati per intercettare le comunicazioni *on-line* di circa mezzo milione di cittadini iraniani: a causa della violazione molti siti governativi *on line* olandesi sono stati disattivati o dichiarati non sicuri da visitare.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

Come rilevato dall'ENISA in un recente rapporto[63], la frequente mancanza di informazione circa le violazioni di dati personali e più in generale circa gli attacchi informatici indirizzati ai vari sistemi di comunicazione elettronica, pubblici e privati, la loro entità e le loro modalità, da un lato non consente all'opinione pubblica di elevare la soglia di attenzione nei confronti di un fenomeno purtroppo in espansione, dall'altro preclude alle autorità pubbliche, alle imprese e agli stessi cittadini/utenti la possibilità di predisporre rimedi efficaci e tempestivi a tutela e protezione di un bene essenziale e delicatissimo (i dati personali), che costituisce uno degli obiettivi della criminalità del terzo millennio.

Nel mese di giugno 2012 uno dei più importanti *social network* del settore professionale esistenti al mondo, ha subito una grave violazione del suo database contenente le *password* di milioni di utenti. In particolare un *file* contenente sei milioni e mezzo di *password* criptate con funzioni di *hash* univoche (algoritmo SHA-1 che trasforma ciascuna parola chiave in un'unica lista di numeri e di lettere), è apparso in un forum *on-line* con sede in Russia. Oltre duecentomila *password* sono state violate. Pur non essendo contenuti nel file i nomi degli utenti o altri dati, cionondimeno i responsabili della sicurezza del predetto *social network* hanno inviato e-mail agli utenti coinvolti, invitandoli a modificare immediatamente le *password*. Le conseguenze di tale intrusione non sono state completamente indicate, cosicché quindi non si può ritenere che sia del tutto eliminato il rischio per i dati personali delle persone interessate.

[63] V. *Cyber Incident Reporting in the EU, loc. cit.*