GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Provvedimenti a carattere generale - 26 luglio 2012

[doc. web n. 1915485]

[comunicato stampa]

Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali - Consultazione pubblica - 26 luglio 2012
(In corso di pubblicazione sulla Gazzetta Ufficiale)

Registro dei provvedimenti
n. 221 del 26 luglio 2012

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti e del dott. Giuseppe Busia, segretario generale;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito "Codice") e, in particolare, l'art. 32-*bis*;

VISTA la direttiva 2002/58/Ce del 12 luglio 2002, del Parlamento europeo e del Consiglio, 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);

VISTA la direttiva 2009/136/Ce del 25 novembre 2009, del Parlamento europeo e del Consiglio, 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;

VISTA la direttiva 2009/140/Ce del 25 novembre 2009, del Parlamento europeo e del Consiglio, 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;

VISTO il decreto legislativo 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"* (pubblicato nella *Gazzetta Ufficiale* 31 maggio 2012 n. 126);

VISTO il decreto legislativo 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"* (pubblicato nella *Gazzetta Ufficiale* 31 maggio 2012, n. 126);

RITENUTO NECESSARIO fornire primi orientamenti e istruzioni in merito ai nuovi obblighi di comunicazione incombenti sui fornitori di servizi di comunicazione elettronica accessibili al pubblico per i casi di violazione di dati personali, come espressamente previsto dall'art. 32-*bis*, comma 6, del Codice;

RILEVATA l'opportunità che la prescrizione di alcune misure, allo stato individuate nell'unito documento, sia preceduta da una consultazione pubblica, diretta in particolare ai predetti fornitori, al fine di acquisire ulteriori riscontri sull'adeguatezza delle medesime prescrizioni, nonché sulle relative modalità attuative, anche in ragione della eventuale casistica che si formerà *medio tempore*;

VISTE le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento n. 1/2000;

RELATORE il dr. Antonello Soro;

DELIBERA

ai sensi degli artt. 32-*bis*, comma 6 e 154, comma 1, lett. *c*), del Codice:

a. di adottare l'unito documento, recante le *"Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali"*, che forma parte integrante della presente deliberazione (Allegato 1).

b. di avviare una consultazione pubblica in merito alle modalità applicative specificate nei punti 4.2, 7.1, 7.2 e 7.3 del documento di cui alla lettera *a*), riservandosi di intervenire sulle stesse anche alla luce delle risultanze delle osservazioni pervenute.

Tali osservazioni e commenti potranno pervenire, **entro il termine di 90 giorni** dalla pubblicazione della presente

deliberazione, all'indirizzo dell'Autorità di Piazza di Monte Citorio n. 121, 00186 Roma, ovvero al seguente indirizzo di posta elettronica:

consultazionedatabreach@gpdp.it

La presente deliberazione verrà pubblicata sul sito *web* del Garante *www.gpdp.it* e sarà trasmessa al Ministero della giustizia ai fini della sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana a cura dell'Ufficio pubblicazione leggi e decreti.

Roma, 26 luglio 2012

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia

Allegato 1

Linee guida in materia di comunicazione delle violazioni di dati personali.

Sommario

1. Considerazioni preliminari.

La direttiva 2002/58/Ce (*c.d. direttiva e-Privacy)* afferma che i fornitori di servizi di comunicazione elettronica devono adottare *"appropriate misure tecniche e organizzative"* per assicurare *"un livello di sicurezza adeguato al rischio esistente"* (art. 4, comma 1). Nella direttiva 2009/136/Ce (che ha modificato la direttiva 2002/58/Ce) si è tenuto conto, in particolare, del fatto che un evento che coinvolga i dati personali, se non trattato in modo adeguato e tempestivo, può provocare un grave danno economico e sociale al contraente (o alle altre persone interessate), tra cui l'usurpazione d'identità (*cfr. considerando 61*).

Con il recepimento delle suindicate previsioni tramite il decreto legislativo 28 maggio 2012, n. 69, con il quale il Governo ha dato attuazione alla delega prevista nell'art. 9 della legge comunitaria del 2010 (legge 15 dicembre 2011, n. 217, pubblicata in G.U. 2 gennaio 2012, n. 1), i fornitori di servizi di comunicazione elettronica sono oggi tenuti a comunicare senza indebiti ritardi al Garante e, in alcuni casi, al contraente o ad altre persone interessate, l'occorrenza dei predetti eventi, qualificati come *"violazioni di dati personali"*.

Le presenti *linee guida* sono volte a fornire –in linea con quanto previsto dalla stessa direttiva 2009/136/Ce indicazioni in merito alla nuova disciplina sopra richiamata, con particolare riguardo alle circostanze in cui i fornitori hanno l'obbligo di comunicare le violazioni di dati personali, al formato applicabile alla comunicazione e alle relative modalità di effettuazione (*cfr.* art. 32-*bis*, comma 6, del Codice).

2. Quadro normativo.

Come sopra accennato, il decreto legislativo 28 maggio 2012, n. 69 ha apportato significative e numerose modifiche al Codice, introducendo, per quanto di specifico interesse, la nuova disciplina concernente la gestione delle suindicate violazioni di sicurezza nel settore delle comunicazioni elettroniche.

È stata così introdotta la definizione di *"violazione di dati personali"*, intesa come la *"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" (art. 4, comma 3, lett. g-*bis*), del Codice).

Si tratta di una definizione da un lato molto ampia, in quanto comprende qualunque evento metta a rischio, anche in maniera del tutto accidentale, i dati trattati nell'ambito dei servizi di comunicazione elettronica, e dall'altro volta a delimitare il contesto (quello, appunto, dei servizi di comunicazione elettronica accessibili al pubblico), nonché l'ambito soggettivo (quello dei fornitori di tali servizi), nel quale opera la nuova disciplina.

In quest'ottica vanno lette anche le modifiche all'art. 32 del Codice, ora espressamente rubricato *"Obblighi relativi ai fornitori di servizi di comunicazione elettronica accessibili al pubblico"* e che impone al fornitore di adottare, anche attraverso altri soggetti cui sia affidata l'erogazione del servizio, *"misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi e per gli adempimenti di cui all'articolo 32-bis"*.

Il legislatore comunitario è peraltro consapevole del fatto che l'interesse degli utenti ad essere informati sulle violazioni di sicurezza che coinvolgono i loro dati personali non si limita al settore delle comunicazioni elettroniche. Ed infatti, le proposte di riforma della legislazione comunitaria in materia di protezione dei dati (*cfr.* schema di Regolamento presentato dalla Commissione europea il 25 gennaio 2012, attualmente all'esame del Parlamento e del Consiglio) prevedono un'estensione generalizzata dell'obbligo di notifica delle violazioni dei dati personali a tutti i titolari pubblici e privati (v. anche considerando 59, direttiva 2009/136/Ce).

In alcuni Stati membri del resto sono già in vigore disposizioni che prevedono una platea più ampia di soggetti che effettuano tale notifica (es. in Irlanda); in tal senso, peraltro, si è espresso anche il Gruppo dei Garanti europei (*c.d. "Gruppo Art. 29"*) nel documento n. 01/2011, adottato il 5 aprile 2011.

Al riguardo, si segnala che il Garante, con il provvedimento del 12 maggio 2011 (pubblicato in G.U. n. 127 del 3 giugno 2011 e disponibile sul sito dell'Autorità, doc. *web* n. 1813953), ha prescritto alle banche, quale misura opportuna, di comunicare tempestivamente all'Autorità –fornendo idonei dettagli– 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.

L'art. 32-*bis* citato introduce poi nel Codice la disciplina degli *"Adempimenti conseguenti ad una violazione di dati personali"* e sancisce l'obbligo, per i fornitori di servizi di comunicazione elettronica accessibili al pubblico, di comunicare senza indebiti ritardi al Garante la violazione di dati personali da essi detenuti. Nei casi in cui dalla violazione possa derivare pregiudizio ai dati personali o alla riservatezza di un contraente o di altra persona, il fornitore dovrà comunicare l'avvenuta violazione anche a tali soggetti (art. 32-*bis*, comma 2).

Tale seconda comunicazione ferma restando la difficoltà, sulla quale si tornerà in seguito, di delimitare i casi nei quali la violazione possa arrecare pregiudizio al contraente o ad altre persone interessate, potendo tale rischio dirsi in astratto sempre sussistente non è dovuta se il fornitore ha dimostrato al Garante di aver utilizzato misure *"che rendono i dati inintelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate al momento della violazione"* (art. 32-*bis*, comma 3). Il Garante, considerate le presumibili ripercussioni negative della violazione, può comunque obbligare il fornitore ad effettuare la predetta comunicazione, ove lo stesso non vi abbia già provveduto (comma 4).

3. Ambito soggettivo.

Come si è già accennato, la nuova disciplina concernente gli obblighi di comunicazione al Garante e alle persone interessate non riguarda la totalità dei titolari dei trattamenti, ossia dei soggetti, pubblici o privati, che detengono e trattano dati personali in funzione della propria attività.

I nuovi adempimenti gravano, infatti, esclusivamente sui fornitori di servizi di comunicazione elettronica accessibili al pubblico e, quindi, su quei soggetti che mettono a disposizione del pubblico, su reti pubbliche di comunicazione, servizi consistenti, esclusivamente o prevalentemente, *"nella trasmissione di segnali su reti di comunicazioni elettroniche"* (art. 4, comma 2, lett. *d*) ed *e*), del Codice).

I medesimi adempimenti sono inoltre connessi alla particolare attività di fornitura dei predetti servizi, quale ad esempio il servizio telefonico o quello di accesso a Internet. Ciò significa che se la violazione riguarda una banca dati del fornitore che non attiene in maniera specifica al servizio offerto dallo stesso, ma ad una qualunque delle altre attività che svolge, ad esempio alla gestione del personale o alla contabilità, l'obbligo di comunicazione non vige.

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), nel quale vi è una sostanziale identità di titolari tenuti alla conservazione ex art. 132 del Codice, nonché all'adozione delle misure ivi prescritte.

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).

Al contrario non rientrano tra tali soggetti:

- coloro 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"*.

- 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;

- i gestori dei siti Internet che diffondono contenuti sulla rete (*c.d. "content provider"*). 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 direttiva 2002/21/Ce cit., esclude essa stessa i *"servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica […]"*;

- i gestori di motori di ricerca.

3.1. 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, prevede che, in questi casi, 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.

Si tratta di una disposizione che riguarda la particolare situazione che vede coinvolti i fornitori di comunicazione elettronica *"tradizionali"* e, ad esempio, i *c.d.* operatori virtuali di rete mobile (*Mobile Virtual Network Operator*, MVNO), ossia le 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 e che utilizzano a tale scopo una parte dell'infrastruttura di uno o più operatori mobili reali (MNO).

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.

Da ciò emerge, pertanto, come gli obblighi di comunicazione derivanti da eventuali violazioni di dati personali dei clienti (o di altre persone interessate) incombano sul MVNO, l'unico a conoscere, nella maggior parte dei casi, l'identità dei clienti stessi. E tuttavia, in ragione del fatto che, come detto, il servizio viene materialmente erogato dal MNO, è necessario che tale soggetto renda noti tutti gli eventi e le informazioni concernenti l'avvenuta violazione all'operatore virtuale, in modo tale che questo possa adempiere ai propri obblighi nei confronti del Garante e, eventualmente, dei clienti.

Al riguardo, si rinvia alle definizioni contenute nella Delibera dell'Autorità per le garanzie nelle comunicazioni n. 544/00/CONS, *"Condizioni regolamentari relative all'ingresso di nuovi operatori nel mercato dei sistemi radiomobili"* (pubblicata in G.U. n. 183 del 7 agosto 2000).

Un altro caso rientrante nella previsione di cui al comma 8 è quello nel quale il fornitore del servizio di comunicazione elettronica, pur potendosi definire "tradizionale", affidi in tutto o in parte la materiale erogazione del servizio stesso a soggetti terzi, che abbiano le infrastrutture a ciò necessarie, ad esempio per ragioni di ottimizzazione dei costi.

Ferma restando la necessità che in tali ipotesi i soggetti coinvolti configurino correttamente i rispettivi ruoli in termini di titolare e responsabile del trattamento, l'eventuale violazione dei dati personali trattati nell'ambito dei sistemi affidati dal fornitore al soggetto terzo, dovrà essere da questo necessariamente comunicata al fornitore stesso entro 24 ore dall'avvenuta conoscenza della violazione, il quale potrà poi comunicare a sua volta la violazione al Garante e, se occorre, al contraente o ad altra persona interessata, come riportato al punto 5.

4. Gestione della sicurezza e delle violazioni.
L'art. 32 del Codice (come modificato dal d.lg. n. 69/2012 in attuazione di quanto previsto dall'art. 4 della direttiva 2002/58/Ce) prevede che i soggetti che operano sulle reti di comunicazione elettronica debbano garantire *"che i dati personali siano accessibili soltanto al personale autorizzato per fini legalmente autorizzati"* (*cfr.* comma 1-*bis*) e che le misure tecniche e organizzative, che il fornitore di comunicazione elettronica deve adottare, siano adeguate al rischio esistente, garantiscano la protezione dei dati archiviati o trasmessi da una serie di eventi espressamente indicati (distruzione, perdita, alterazione, anche accidentali, archiviazione, trattamento, accesso o divulgazione non autorizzati o illeciti) e assicurino l'attuazione di una *"politica di sicurezza"* (*cfr*. comma 1-*ter*).

Il nuovo art. 32, comma 3, infine, impone al fornitore di informare i contraenti, il Garante, l'Agcom e, ove possibile, gli utenti, dell'esistenza di *"un particolare rischio di violazione della sicurezza della rete"*, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle suindicate misure, tutti i possibili rimedi e i relativi costi presumibili.

Tali previsioni indicano chiaramente come i fornitori siano tenuti ad organizzarsi al proprio interno al fine di garantire un elevato livello di sicurezza dei dati detenuti e gestire in maniera strutturata e tramite procedure e interventi definiti a priori, le eventuali violazioni di dati personali che dovessero accadere.

Come dichiarato anche dall'ENISA nelle sue recenti Raccomandazioni (disponibili all'indirizzo *http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech*), la gestione del rischio, in primo luogo, e delle violazioni di dati personali, qualora dovessero verificarsi, non può essere affidata dai fornitori a un'attività estemporanea. Essa richiede la predisposizione di un idoneo piano, nel quale dovrà essere individuata una serie di misure tecniche e organizzative di livello commisurato al tipo di minaccia, in grado di garantire risposte tempestive, efficaci e adeguate all'entità della violazione.

Quanto all'individuazione delle misure minime di sicurezza propriamente dette ossia quelle alle quali la legge riconduce sanzioni di carattere anche penale ex art. 169 del Codice si richiama l'art. 33 del Codice e le specifiche previsioni contenute nel Disciplinare tecnico in materia di misure minime di sicurezza, di cui all'Allegato B (in particolare quelle relative ai trattamenti svolti con strumenti elettronici), la cui adozione è peraltro obbligatoria per qualunque titolare del trattamento.

4.1. Analisi dei rischi.
Al fine di ottemperare agli obblighi di cui all'art. 32 del Codice, è necessario che i fornitori effettuino una preliminare ricognizione dell'insieme dei dati personali trattati e dei rischi ai quali gli stessi vanno incontro.

È necessario, quindi, che ciascun fornitore identifichi e attribuisca un valore ai differenti dati personali che detiene e ai pericoli cui gli stessi sono esposti, individuando la propria soglia di accettazione dei rischi e fissando le opportune strategie di gestione. Il fornitore è anche tenuto a individuare delle soglie di rischio, ad esempio in base a livello basso, medio e alto, in ragione delle quali decidere non solo quali misure adottare per garantire un'idonea protezione dei dati detenuti, ma anche se effettuare la comunicazione al contraente o alle altre persone interessate.

Tale preliminare ricognizione consentirà ai fornitori di predisporre misure di sicurezza volte sia a prevenire i possibili eventi dannosi, sia a intervenire nel momento in cui gli stessi dovessero comunque –nonostante le misure adottate verificarsi.

Si tratta di valutazioni sostanzialmente analoghe a quelle che i fornitori, sino al 10 febbraio scorso, erano tenuti ad effettuare ai fini della redazione del Documento programmatico sulla sicurezza, misura minima prevista dalla regola 19 del richiamato Disciplinare tecnico, abrogata dall'art. 45, comma 1, lett. d), del decreto legge 9 febbraio 2012, n. 5 (convertito, con modificazioni, dalla legge 4 aprile 2012, n. 35).

4.2. Adozione di adeguate misure di sicurezza (in consultazione).
L'analisi dei rischi sopra indicata è alla base della predisposizione, da parte dei fornitori, delle misure di sicurezza *"adeguate al rischio esistente"*, richiamate dal nuovo art. 32, comma 1, del Codice, nonché dell'individuazione di quelle maggiormente in grado di porre rimedio alla violazione eventualmente verificatasi, le quali peraltro debbono essere descritte al Garante nella comunicazione, come previsto dall'art. 32-*bis*, comma 5, del Codice.

Si adottano in particolare, le seguenti misure in grado di garantire un livello minimo comune di sicurezza:

1. rendere i dati trattati immediatamente non disponibili per ulteriori elaborazioni da parte di sistemi informativi al termine delle attività svolte e nelle quali gli stessi sono coinvolti, provvedendo alla loro cancellazione o trasformazione in forma anonima in tempi tecnicamente compatibili con l'esercizio delle relative procedure informatiche, nei data base e nei sistemi di elaborazione utilizzati per i trattamenti, nonché nei sistemi e nei supporti per la realizzazione di copie di sicurezza (*backup* e *disaster recovery*), anche con il ricorso a tecnologie crittografiche o di anonimizzazione;

2. adottare soluzioni informatiche idonee ad assicurare la possibilità di controllo delle attività svolte sui dati da ciascun incaricato del trattamento, quali che siano la sua qualifica, le sue competenze, gli ambiti di operatività e le finalità del trattamento. Il controllo deve essere efficace e dettagliato anche per i trattamenti condotti sui singoli elementi di informazione presenti sui diversi *database* utilizzati;

3. porre particolare attenzione ai dispositivi portatili, predisponendo specifiche misure di sicurezza in grado di mitigare il rischio connesso alla portabilità dell'apparato, e di assicurare agli stessi un livello di sicurezza analogo a quello applicato agli altri dispositivi informatici, in considerazione del fatto che molto spesso le violazioni della sicurezza riguardano i dispositivi mobili utilizzati da dipendenti e collaboratori dei fornitori al di fuori degli uffici delle aziende.

5. Comunicazione al Garante: tempi e contenuto.
La predisposizione da parte dei fornitori di un idoneo piano di gestione delle violazioni sulla base di un'accurata analisi dei rischi è necessaria per poter adempiere correttamente anche all'obbligo di comunicazione al Garante previsto dall'art. 32-*bis*. Tale disposizione stabilisce infatti che il fornitore debba comunicare la violazione dei dati personali al Garante *"senza indebiti ritardi"*, ossia nel momento in cui lo stesso ne viene a conoscenza.

Stante l'importanza della tempestività della comunicazione al Garante, ma considerando anche la complessità e il numero dei sistemi in uso presso i fornitori, nonché dei dati che detengono, si ritiene che tali soggetti nelle situazioni più articolate possano, in un primo momento, limitarsi a fornire all'Autorità sommarie informazioni in relazione alla violazione verificatasi, purché ciò avvenga immediatamente dopo l'avvenuta conoscenza della stessa, integrando poi la comunicazione in un momento successivo.

Tali sommarie informazioni devono in ogni caso consentire all'Autorità di effettuare una prima valutazione dell'entità della violazione e devono, quindi, comprendere:

- i dati identificativi del fornitore;
- una breve descrizione della violazione;
- l'indicazione della data anche presunta della violazione e del momento della sua scoperta;
- l'indicazione del luogo in cui è avvenuta la violazione dei dati, anche nel caso in cui essa sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili;
- l'indicazione della natura e del contenuto dei dati anche solo presumibilmente coinvolti;
- una sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

Si ritengono congrui, quali termini entro i quali provvedere alla comunicazione, quello di 24 ore dall'avvenuta conoscenza della violazione per la prima sommaria comunicazione, e quello di 3 giorni dalla stessa per la comunicazione dettagliata. Per agevolare l'adempimento, è stato predisposto un modello di comunicazione da inviare al Garante, disponibile *on line* sul sito dell'Autorità e idoneo alla raccolta delle informazioni sulla violazione nonché al loro successivo trattamento con strumenti informatici da parte del Garante.

Quanto al contenuto della comunicazione, l'art. 32-*bis*, comma 5, del Codice prevede che essa, oltre alla descrizione della natura della violazione, all'indicazione dei punti di contatto presso cui ottenere maggiori informazioni e all'elenco delle misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione (elementi da inserire anche nell'eventuale comunicazione ai soggetti interessati), descriva le conseguenze della violazione e le misure proposte o adottate dal fornitore per porvi rimedio.

Qualora, all'esito delle verifiche effettuate dal fornitore successivamente alla prima sommaria comunicazione, non dovessero emergere ulteriori elementi, il fornitore dovrà comunicare al Garante le modalità con le quali ha posto rimedio alla violazione e le misure adottate per prevenire ulteriori violazioni della medesima specie.

In sostanza, è necessario che dalla comunicazione emergano gli elementi dai quali l'Autorità possa valutare compiutamente la gravità dell'evento verificatosi, anche in ragione del numero dei soggetti coinvolti e della quantità e qualità dei dati colpiti, l'entità del danno cagionato e le misure adottate per ridurlo. Ciò, al fine di intervenire con le prescrizioni che si rendessero necessarie, compresa quella di comunicare l'avvenuta violazione ai contraenti o alle altre persone interessate.

Parimenti importante, al fine di consentire all'Autorità di svolgere eventuali accertamenti, risulta l'indicazione, nella comunicazione, dei sistemi applicativi colpiti dalla violazione, nonché l'ubicazione fisica dei sistemi di elaborazione impiegati nel trattamento.

L'obbligo di comunicare l'avvenuta violazione al Garante ed eventualmente al contraente (o ad altra persona interessata) sussiste, ovviamente, anche qualora l'evento abbia interessato dispositivi mobili e indipendentemente dal fatto che sugli stessi siano installati sistemi di protezione dei dati. Anche per tali dispositivi (come si vedrà nel prosieguo) l'unica ipotesi in cui il fornitore può esimersi dalla comunicazione al contraente (o ad altra persona interessata) è quella in cui i dati in essi contenuti o tramite gli stessi accessibili siano stati resi inintelligibili.

6. Inventario delle violazioni di dati personali.

Al medesimo scopo, quello cioè di consentire al Garante di svolgere il proprio compito di controllo sul rispetto, da parte dei fornitori, delle disposizioni in materia di violazione dei dati personali, è finalizzata la previsione relativa alla tenuta di un inventario aggiornato delle violazioni, di cui all'art. 32-*bis*, comma 7, del Codice (*cfr.* anche considerando 58, direttiva 136/2009/Ce).

In tale inventario, i fornitori devono inserire tutte (e soltanto) le informazioni necessarie a chiarire le circostanze nelle quali si sono verificate le violazioni, le conseguenze che le stesse hanno avuto e i provvedimenti adottati per porvi rimedio.

L'inventario dovrà essere continuamente aggiornato dai fornitori e messo a disposizione del Garante, qualora l'Autorità chieda di accedervi. Dovranno, inoltre, essere adottate dal fornitore idonee misure atte a garantire l'integrità e l'immodificabilità delle registrazioni in esso contenute.

7. Comunicazione al contraente o ad altre persone.

Qualora si verifichi una violazione di dati personali e dalla stessa possa derivare un pregiudizio ai dati personali o alla riservatezza di un contraente o di altre persone, ossia dei soggetti ai quali si riferiscono i dati violati, oltre alla comunicazione al Garante, i fornitori sono tenuti a comunicare l'avvenuta violazione, senza ritardo, anche a tali soggetti (art. 32-*bis*, comma 2, del Codice).

In questo caso, si ritiene che il fornitore debba procedere alla suindicata comunicazione non oltre il termine di 3 giorni dall'avvenuta conoscenza della violazione. Il fornitore potrà poi scegliere il canale di comunicazione che riterrà più idoneo, tenendo conto di quanto indicato nel successivo punto 7.2.

La predetta comunicazione non è dovuta se il fornitore è in grado di dimostrare al Garante di aver applicato ai dati oggetto della violazione misure tecnologiche di protezione che li hanno resi inintelligibili a chiunque non sia autorizzato ad accedervi (cfr. art. 32-*bis*, comma 3, del Codice), ad esempio, tramite tecniche di cifratura.

In ogni caso, in ragione dell'entità del possibile pregiudizio per gli interessati, devono essere sempre comunicate immediatamente ai contraenti le violazioni che riguardano le credenziali di autenticazione (nome utente e password, ancorché quest'ultima sia cifrata o sottoposta a funzioni di hashing) o le chiavi di cifratura utilizzate dai contraenti medesimi.

7.1. Inintelligibilità dei dati (in consultazione).

A giudizio dell'Autorità, si considerano inintelligibili i dati che, ad esempio:

a. siano stati cifrati in modo sicuro attraverso un algoritmo standardizzato, purché la chiave di decifrazione non sia stata compromessa da violazioni della sicurezza e sia stata generata in modo da non consentirne la derivazione con gli strumenti tecnologici disponibili da parte di soggetti non autorizzati ad accedervi; oppure

b. siano stati sostituiti da un valore di *hash* calcolato attraverso una funzione crittografica di *hashing* a chiave, purché la chiave utilizzata per effettuare lo *hashing* dei dati non sia stata compromessa da violazioni della sicurezza e sia stata generata in modo da non consentirne la derivazione con gli strumenti tecnologici disponibili da parte di soggetti non autorizzati ad accedervi; oppure

c. siano stati resi anonimi con procedure tali da rendere praticamente impossibile la reidentificazione degli interessati cui si riferiscono da parte di soggetti non legittimati al loro trattamento.

In ragione del fatto che, astrattamente, il rischio che una violazione di dati personali arrechi pregiudizio ai dati stessi o alla riservatezza dei soggetti ai quali essi si riferiscono è sempre sussistente, non è certamente semplice definire a priori in quali casi il fornitore possa esimersi dall'effettuare la comunicazione della violazione al contraente o alle altre persone interessate.

L'art. 32-*bis*, comma 4, del Codice prevede comunque che, ove il fornitore non vi abbia provveduto, il Garante, considerate le presumibili ripercussioni negative della violazione, può obbligare lo stesso ad effettuare la comunicazione al contraente o ad altra persona interessata. È evidente che tale possibilità prescinde dal fatto che il fornitore abbia reso inintelligibili i dati violati: tale evenienza riduce, non fa venir meno, il rischio che i dati violati siano comunque decifrabili e che, pertanto, il Garante imponga di effettuare comunque la comunicazione.

Da quanto detto, risulta di tutta evidenza la necessità che il fornitore dia conto, nella comunicazione al Garante, della politica di sicurezza attuata e che descriva anche le conseguenze della violazione verificatasi e le misure proposte o adottate per porvi rimedio, in tal modo consentendo all'Autorità di fare le proprie valutazioni e dare eventuali prescrizioni.

7.2. Canale per la comunicazione al contraente o ad altre persone (in consultazione).
Ciascun fornitore dovrà valutare quale sia il canale di comunicazione che consente di raggiungere più facilmente e tempestivamente i soggetti i cui dati sono interessati dalla violazione. E ciò, sia con riguardo ai contraenti, sia, soprattutto, con riferimento a quelle persone che non sono clienti del fornitore, ma che pure sono state coinvolte dalla violazione.

In determinate circostanze, soprattutto con riferimento ai soggetti da ultimo indicati, ma anche in relazione ai clienti del fornitore, nei casi in cui sia coinvolto un numero molto elevato di contraenti, si ritiene che il medesimo fornitore possa più facilmente raggiungere lo scopo previsto dalla normativa informare senza ritardo i soggetti i cui dati sono coinvolti dalla violazione tramite forme di comunicazione diverse da quella *ad personam*.

Si ritiene, cioè, che in alcuni casi siano più utili forme di comunicazione di carattere pubblico, quali la diffusione di avvisi su quotidiani, anche online, oppure per mezzo di emittenti radiofoniche, anche locali. Tali forme alternative di comunicazione ai contraenti o alle altre persone coinvolte dalla violazione vanno ovviamente realizzate anch'esse entro il più breve lasso di tempo e, comunque, entro il termine di 3 giorni indicato ai punti 5 e 7.

7.3. Valutazione del rischio che richiede la comunicazione al contraente o ad altre persone (in consultazione).
Come si è detto, è necessario che il fornitore effettui delle valutazioni per decidere quali misure adottare per ridurre il rischio, attenuare il danno qualora si verifichi la violazione e decidere se comunicare al contraente e/o alle altre persone, consentendo loro, così, di adottare le precauzioni necessarie.

Tali valutazioni dovrebbero essere svolte sulla base di criteri determinati e comuni a tutti i fornitori, in modo tale da porre in campo scelte ponderate e confrontabili. Potrebbero soccorrere, ai fini della suindicata valutazione, innanzitutto elementi quali la quantità e la qualità dei dati coinvolti nella violazione.

A titolo meramente esemplificativo, una violazione che riguardi un solo dato personale o, anche, più dati personali, non sensibili, di un solo contraente ferma restando la necessità che il fornitore adotti tutte le misure in grado di ridurre il danno potrebbe non dover essere necessariamente comunicata allo stesso ai sensi dell'art. 32-bis, comma 2.

Parimenti importante e, dunque, da considerare nella valutazione del rischio, è la "attualità" dei dati detenuti, ossia il tempo trascorso dall'acquisizione dei dati stessi e dal loro inserimento nei database del fornitore. Dati più recenti potrebbero infatti destare maggiore interesse per eventuali malintenzionati in quanto è più alta la probabilità che essi esprimano in modo attendibile uno "stato" o una specifica condizione (economica, di salute, abitativa ecc.) in cui si trova l'interessato al momento dell'avvenuta violazione.

Potrebbe essere utile poi, per decidere se comunicare o meno la violazione agli interessati, considerare gli effetti della violazione stessa e ritenere sussistente il pregiudizio per i dati o la vita privata del contraente o di altra persona quando la violazione *"implica, ad esempio, il furto o l'usurpazione d'identità, il danno fisico, l'umiliazione grave o il danno alla reputazione in relazione con la fornitura di servizi di comunicazione*" (*cfr.* considerando 61, direttiva 2009/136/Ce).

Per giungere a valori uniformi e comparabili, i fornitori dovrebbero affrontare la valutazione del rischio anche con un approccio di tipo quantitativo, individuando in ragione dei succitati attributi dei dati coinvolti nella violazione (qualità, quantità, attualità, ecc.), specifiche metriche in grado di rappresentare gli effetti pregiudizievoli che la stessa potrebbe provocare sull'interessato.

8. Conseguenze per le ipotesi del mancato rispetto dei nuovi obblighi di sicurezza.
Per le ipotesi di violazione dei nuovi obblighi di sicurezza, il d.lg. n. 69/2012 ha introdotto nel Codice nuove e specifiche sanzioni amministrative (*cfr.* art. 162-*ter*) ed ha esteso quella penale prevista dall'art. 168 all'ipotesi di falsità nelle notificazioni al Garante ai sensi dell'art. 32-*bis*, commi 1 e 8.

L'art. 162-*ter* stabilisce che la omessa o ritardata comunicazione della violazione di dati personali al Garante ex art. 32-*bis*, comma 1, è punita con la sanzione amministrativa del pagamento di una somma da venticinquemila euro a centocinquantamila euro; la omessa o ritardata comunicazione della violazione di dati personali al contraente o ad altra persona ex 32-*bis*, comma 2, è punita con la sanzione amministrativa del pagamento di una somma da centocinquanta euro a mille euro per ciascun contraente o altra persona interessata.

In tale ipotesi, poi, il fornitore non può beneficiare del cumulo giuridico di cui all'art. 8 della legge n. 689/1981 e, tuttavia, la sanzione non può essere applicata in misura superiore al 5 per cento del volume d'affari realizzato dallo stesso nell'ultimo esercizio chiuso anteriormente alla notificazione della contestazione della violazione amministrativa, ferma restando la possibilità di aumento fino al quadruplo se le sanzioni risultino inefficaci in ragione delle condizioni economiche del contravventore, ai sensi dell'art. 164-*bis*, comma 4 (*cfr.* art. 162-*ter*, commi 2 e 3).

Ai sensi dell'art. 162-*ter*, comma 4, la violazione della disposizione concernente la tenuta di un aggiornato inventario delle violazioni di dati personali, è punita con la sanzione amministrativa del pagamento di una somma da ventimila euro a centoventimila euro.

Le medesime sanzioni previste per i fornitori si applicano anche nei confronti dei soggetti ai quali sia stata affidata l'erogazione dei servizi, qualora tali soggetti abbiano omesso di comunicare senza ritardo al fornitore tutte le informazioni necessarie allo stesso per adempiere ai propri obblighi (art. 162-*ter*, comma 5).

L'art. 168 punisce, infine, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni il fornitore che dichiari o attesti falsamente notizie o circostanze, o produca atti o documenti falsi in occasione della comunicazione al Garante conseguente alla violazione di dati personali, nonché i soggetti, cui sia affidata l'erogazione del servizio, che effettuino false comunicazioni al fornitore.

stampa **chiudi**