Autorità Amministrative Indipendenti

a cura di

Giovanna De Minico

***

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

di *Antonietta Rubino*

aggiornato al 19.06.2012

Nel periodo di riferimento, il Garante per la protezione dei dati personali ha adottato due autorizzazioni generali: Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso la Nuova Zelanda, (G. U. 78 del 3 aprile 2013); Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso la Repubblica orientale dell'Uruguay, (G. U. n. 78 del 3 aprile 2013), a seguito delle decisioni della Commissione europea (2013/65/UE per la Nuova Zelanda e 2012/484/UE per la Repubblica orientale dell'Uruguay) che hanno accertato l'adeguatezza della tutela dei dati personali al fine di consentire il trasferimento dall'Unione europea.

Di notevole interesse è il "Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. *data breach*)", pubblicato sulla G.U. n. 97 del 4 aprile 2013.

Con la Direttiva 2009/136/CE è stata innovata la 2002/58/CE, apportando delle modifiche che riguardano, tra l'altro, la sicurezza dei dati e le procedure da adottare in caso di violazione dei dati.

Una prima novità del testo comunitario, recepito col d.lgs. 69/2012, è la definizione di "violazione di dati personali", intesa come "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, definizione sostanzialmente sovrapponibile a quella dell'art. 2, comma 2, lett. c, della Direttiva).

L'obbligo è riferibile solo ai fornitori dei servizi di comunicazione accessibili al pubblico, individuati dal Garante mediante il richiamo al provvedimento *data retention* (provv. del 17 gennaio 2008), con la conseguente esclusione, quindi, di coloro che offrono servizi a un gruppo limitato di persone, dei titolari e i gestori di esercizi pubblici e di circoli privati che mettono a disposizione del pubblico terminali per le comunicazioni, dei *content provider*, dei gestori dei motori di ricerca.

Nel caso in cui il fornitore affidi l'erogazione del servizio a soggetti terzi, questi devono comunicargli tutte le informazioni necessarie per adempiere agli oneri previsti in caso di violazione dei dati.

La novella normativa prevede, all'art. 32 del Codice, che il fornitore debba informare i contraenti, il Garante e l'Agcom dell'esistenza di particolari rischi di violazione della rete. Propedeutica a tale adempimento è l'analisi preventiva cui è tenuto il fornitore con una valutazione dei pericoli e delle eventuali misure di sicurezza, analogamente a ciò che avveniva col la predisposizione del DPS, non più obbligatorio dopo l'abrogazione dell'art. 45, comma 1, lett. d, ad opera del d.l. 5 del 9 febbraio 2012.

Rispetto a tali misure di sicurezza, il Garante suggerisce, senza vincolare, di rendere i dati trattati immediatamente non disponibili dopo le attività in cui sono utilizzati, attraverso la cancellazione e l'anonimizzazione e di prestare particolare attenzione ai dispositivi mobili, adottando misure specifiche di sicurezza che tengano conto della portabilità dell'apparato.

Di diverso tenore le disposizioni relative alle comunicazioni da effettuare al Garante in caso di violazione dei dati, perché l'Autorità prescrive quali informazioni devono essere trasmesse (dati del fornitore, descrizione della violazione, data anche presunta, luogo, natura e tipologia dei dati coinvolti, descrizione dei sistemi di elaborazione e memorizzazione utilizzati). Il termine previsto è di 24 ore dall'avvenuta conoscenza par la comunicazione sommaria, di tre giorni per quella dettagliata.

Nella comunicazione, oltre alla descrizione dei fatti, devono essere indicate le conseguenze e le misure predisposte per rimediare alla violazione. L'accuratezza deve essere tale da permettere al Garante di vagliare la gravità delle circostanze, anche in ragione del numero di utenti coinvolti, della quantità e della tipologia dei dati. Al fine di

permettere il controllo del Garante, i fornitori devono tenere un inventario in cui riportare gli avvenimenti, le violazioni e i provvedimenti adottati.

La comunicazione, nel caso in cui il fornitore non abbia superato il vaglio del Garante in merito alle misure adottate per rendere intelligibili i dati, deve essere rivolta, individualmente o, se la violazione riguarda più soggetti, tramite quotidiani o emittenti radiofoniche, anche al contraente o agli altri soggetti cui si riferiscono i dati. L'intelligibilità dei dati può essere assicurata, secondo l'Autorità, attraverso sistemi di cifratura o di anonimizzazione.

Una fase essenziale nella procedura è l'individuazione del rischio che, si legge nel provvedimento, dovrebbe avvenire sulla base di criteri determinati e comuni. Anche in questo caso, l'Autorità suggerisce, senza imporre, i parametri da utilizzare per l'analisi dei pericoli, potendo tener conto delle misure di sicurezza già in essere, della tipologia dei dati, delle possibili violazioni, dell'identificabilità dei contraenti, dell'attualità dei dati.

In conclusione, si descrive il quadro sanzionatorio in caso di mancato rispetto dei nuovi obblighi di sicurezza, applicabile ai fornitori e ai soggetti cui eventualmente è affidata l'erogazione dei servizi. Ai sensi dell'art. 162 ter, è punita l'omessa comunicazione al Garante della violazione dei dati, con una somma da venticinquemila a centocinquantamila euro, mentre nel caso in cui non si sia provveduto a informare i contraenti interessati, è previsto il pagamento di una somma da centocinquanta a mille euro. In quest'ultimo caso non si può godere del beneficio del cumulo ma sussiste il limite del cinque per cento del volume di affari come soglia limite e la possibilità di quadruplicare la sanzione se dovesse risultare inefficace.

La violazione della disposizione relativa all'inventario è punita, ex art. 162 ter, comma 4, con una sanzione da ventimila a centoventimila euro.

La più grave sanzione, ai sensi dell'art. 168 che prevede la reclusione da sei mesi a tre anni, è comminata nel caso in cui il fornitore dichiari o attesti false notizie, o produca falsi documenti in occasione della comunicazione al Garante e nel caso in cui il soggetto erogatore effettui false comunicazioni al fornitore.