# DATA BREACH E OBBLIGHI DI LEGGE:
# LE NUOVE REGOLE PER OPERATORI TELEFONICI E INTERNET PROVIDERS

di Luca Giacopuzzi[1]

Il decreto legislativo 28 maggio 2012 n.69 ha apportato significative modifiche al Codice in materia di protezione dei dati personali ("il Codice"), introducendo, per quanto di interesse ai fini del presente contributo, una nuova disciplina in tema di "*data breach*", dettata dagli articoli 32 e 32-bis del Codice. La portata delle nuove prescrizioni è precisata da "Linee Guida"[2] del Garante per la protezione dei dati personali ("il Garante"), che forniscono significative istruzioni per l'esatta comprensione di una materia per il vero non priva di elementi di criticità. Il presente lavoro si propone di illustrarne al lettore il quadro normativo e di offrire al predetto una sorta di "bussola" per orientarsi tra i numerosi precetti, al fine di meglio individuare gli adempimenti da porre in essere.

Le recenti modifiche all'art. 32 del Codice hanno sensibilmente innovato gli obblighi in tema di sicurezza informatica che gravano sui fornitori di servizi di comunicazione elettronica accessibili al pubblico, ridisegnandone i confini normativi. Le previsioni ivi previste denotano come i fornitori siano tenuti a (ri)organizzarsi al proprio interno, per presidiare più efficacemente la sicurezza dei dati oggetto di trattamento, sì da essere in grado di gestire tramite procedure e interventi definiti a priori le eventuali violazioni di dati personali, di cui si dirà.

Il primo comma dell'art. 32 del Codice, in particolare, 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'art. 32-bis". Il che comporta, di necessità, l'ulteriore onere di effettuare una preliminare ricognizione dell'insieme dei dati trattati e dei rischi ai quali i fornitori vanno incontro, atteso che l'analisi dei rischi pare ineludibile al fine di ottemperare agli obblighi di cui all'art. 32 del Codice. Indugiare sull'individuazione delle misure di sicurezza da adottare in concreto ci porterebbe fuori strada; al proposito, tuttavia, non pare inopportuno rammentare come sia necessario porre particolare attenzione al presidio dei

[1]Avvocato in Verona (www.lucagiacopuzzi.it), titolare dello Studio Legale Giacopuzzi – Diritto d'Impresa (www.studiogiacopuzzi.it).

[2] Trattasi del Provvedimento a carattere generale del 26 luglio 2012, recante le "Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali".

dispositivi mobili, predisponendo specifici accorgimenti in grado di controbilanciare il maggior rischio connesso, di *default*, alla portabilità dell'apparato (e ciò, se del caso, facendo ricorso anche a tecnologie crittografiche o di anonimizzazione dei dati ivi residenti).

I più significativi precetti che i fornitori di servizi di comunicazione elettronica accessibili al pubblico devono osservare sono partitamente enunciati dall'art.32-bis, norma la cui portata, come anticipato, viene precisata dalle Linee Guida: una lettura coordinata delle relative disposizioni è la chiave per comprendere la nuova disciplina dettata in tema di violazione di dati personali e, in particolare, degli obblighi di comunicazione che ne costituiscono il tratto caratterizzante.

Prima di procedere oltre (e di prendere singolarmente in rassegna gli adempimenti conseguenti ad un episodio di *data breach*), preme chiarire il significato di "violazione di dati personali", locuzione della quale vi è una definizione normativa. L'art. 4, comma 3, lett. g-bis, infatti, precisa che per "violazione di dati personali" si intende 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". Si tratta di una definizione che, sebbene molto ampia (in quanto comprende qualsiasi evento metta a rischio, anche accidentalmente, i dati trattati nell'ambito dei servizi di comunicazione elettronica), allo stesso tempo è volta a delimitare il contesto, oggettivo (quello, appunto, dei servizi di comunicazione elettronica accessibili al pubblico) e soggettivo (quello dei fornitori dei predetti servizi), nel quale opera la nuova disciplina.

Proprio in ordine all'ambito soggettivo di applicazione giova ora soffermarci, al fine di sgombrare il campo da equivoci di sorta.

Come già si è accennato, i nuovi adempimenti gravano unicamente sui fornitori di servizi di comunicazione elettronica accessibili al pubblico e dunque, giusta definizione di legge, su coloro che mettono a disposizione del pubblico, su reti pubbliche di comunicazione, servizi consistenti nella trasmissione di segnali su reti di comunicazioni elettroniche.

Tra i predetti rientrano le società telefoniche e i fornitori di servizi di accesso a Internet (cd. access providers), ma non coloro che offrono servizi di comunicazione elettronica a gruppi delimitati di individui, i titolari e i gestori di esercizi pubblici o di circoli privati, i gestori dei siti Internet che diffondono contenuti in rete (cd. content providers) o dei motori di ricerca.

Le Linee Guida del Garante, peraltro, precisano efficacemente che gli obblighi di legge attengono alla particolare natura dei servizi in parola, di talchè, se la violazione dei dati

personali ha ad oggetto una banca dati del fornitore non strettamente correlata a detti servizi, gli adempimenti di cui all'art. 32-bis non devono aver luogo. La norma testè citata prende espressamente in considerazione l'ipotesi in cui il fornitore presti il servizio di comunicazione elettronica in outsourcing, affidandone l'erogazione a terzi. Ciò accade tipicamente vuoi per scelta (in particolare per ottimizzare i costi d'esercizio) vuoi, per così dire, per necessità; trattasi, in quest'ultimo caso, della situazione dei cd. operatori virtuali di rete mobile (Mobile Virtual Network Operator, MVNO), ossia di quei soggetti che forniscono servizi di telefonia senza possedere alcuna licenza per il relativo spettro radio né tutte le infrastrutture necessarie per fornire tali servizi e che utilizzano all'uopo una parte dell'infrastruttura di uno o più operatori reali di rete mobile (Mobile Network Operator, MNO). Per entrambe le ipotesi sopra considerate trova applicazione il comma 8 dell'art. 32-bis, che, al verificarsi di una violazione di dati personali, grava gli outsourcers dell'obbligo di comunicare "senza indebito ritardo al fornitore tutti gli eventi e le informazioni necessarie a consentire a quest'ultimo di effettuare gli adempimenti" prescritti dal Codice.

Ciò premesso in ordine all'ambito soggettivo di applicazione della disciplina in tema di violazione di dati personali, preme, a questo punto, illustrare gli adempimenti che a detta violazione conseguono, i quali, come innanzi osservato, sono dettati dall'art. 32-bis. I primi due commi della norma testè citata sono assai significativi, poiché il legislatore affida ad essi il compito di stabilire quando una violazione di dati personali deve essere comunicata unicamente al Garante e quando lo deve essere, altresì, agli utenti. Il primo di essi così recita: "In caso di violazione di dati personali, il fornitore di servizi di comunicazione elettronica accessibili al pubblico comunica senza indebiti ritardi detta violazione al Garante". Il secondo così prosegue: "Quando la violazione di dati personali rischia di arrecare pregiudizio ai dati personali o alla riservatezza del contraente o di altra persona, il fornitore comunica anche agli stessi senza ritardo l'avvenuta violazione". A ben vedere, i precetti in esame appaiono mal formulati, in quanto 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 (e, dunque, stando al dato letterale, la comunicazione di cui al secondo comma dovrebbe essere sempre dovuta). La considerazione che precede è tuttavia probabilmente speciosa, in quanto le Linee Guida hanno chiarito che la comunicazione agli utenti è da effettuarsi solo nei casi più gravi, sui quali si tornerà.

Nel trattare della comunicazione al Garante (riferendo, in particolare, dei tempi in cui detta va effettuata) è da rimarcare che, per espressa disposizione di legge, il fornitore deve comunicare la violazione dei dati personali "senza indebiti ritardi". Anche in tal caso da un punto di vista strettamente lessicale la norma non pare immune da censure, poiché "senza indebiti ritardi" è locuzione troppo vaga. Soccorrono, una volta ancora, le Linee Guida, che prevedono che per adempiere all'obbligo di cui al comma 1 dell'art.32-bis del Codice il fornitore debba comunicare la violazione dei dati personali nel momento stesso in cui ne viene a conoscenza. In ragione del fatto che, almeno nelle situazioni più articolate, la ricognizione dell'evento e l'analisi delle conseguenze sono operazioni che non si esauriscono in tempi brevi, il Garante precisa opportunamente che i fornitori possono limitarsi a fornire all'Autorità, entro 24 ore dall'avvenuta conoscenza della violazione, sommarie informazioni cui poi far seguire, entro 3 giorni dal medesimo termine, una relazione più dettagliata, che, 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 menzionare anche nell'eventuale comunicazione agli utenti), indichi le conseguenze della violazione e le misure proposte o adottate dal fornitore per porvi rimedio, come richiesto dal comma 5 della disposizione in esame.

Sempre per ciò che attiene al contenuto della comunicazione, non va taciuta l'importanza di indicare nella predetta, in aggiunta a quanto precede, i sistemi applicativi violati nonché la relativa ubicazione fisica, atteso che trattasi di informazioni preziose per permettere al Garante una compiuta valutazione della gravità del evento.

Già si è detto che, qualora si verifichi una violazione di dati personali da cui può conseguire un rischio di pregiudizio per i dati medesimi o per la riservatezza degli interessati (leggasi, come parimenti già osservato, "nei casi più gravi"), oltre alla comunicazione al Garante gli operatori telefonici e gli Internet providers sono tenuti, ai sensi del comma 2 dell'art.32-bis del Codice, a comunicare la violazione anche a tali individui, senza ritardo. Nel chiarire il significato dell'espressione "senza ritardo", le Linee Guida utilizzano il metro già impiegato in relazione alla locuzione "senza indebito ritardo" di cui al comma 1, e, pertanto, specificano che il fornitore deve procedere alla comunicazione agli utenti nel termine di 3 giorni dall'avvenuta conoscenza della violazione.

Salvo ritenere che la predetta comunicazione sia dovuta in ogni ipotesi di violazione di dati personali (il che, come abbiamo notato, nonostante il non felice dato letterale del comma

2, è una conclusione da ripudiare) rimane da chiarire quali siano le gravi violazioni che fanno sorgere l'obbligo di comunicazione in esame. Definirle a priori non è agevole, e il Garante esce dall'*impasse* ammonendo i fornitori sulla necessità che, a tal fine, prendano in esame, quale criterio orientativo, anzitutto la quantità e la qualità dei dati coinvolti nella violazione (dati finanziari, sanitari, giudiziari, ecc.). Altro parametro importante è l'attualità dei dati, atteso che i dati più recenti destano maggior interesse per i malintenzionati, in quanto più idonei ad esprimere in modo attendibile la condizione in cui versa l'interessato al momento della violazione. Non è inopportuno, infine, considerare gli effetti della violazione, e ritenere sussistente il pregiudizio per i dati o la vita privata degli utenti quando dalla violazione stessa può conseguire il furto d'identità, il danno fisico o il danno alla reputazione.

Va detto, peraltro, che, per espressa previsione di legge, la comunicazione di cui al comma 2 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 inintellegibili a chiunque non sia autorizzato ad accedervi (per esempio, mediante il ricorso a tecniche di cifratura).

Della norma ora in commento (l'art. 32-bis del Codice) rimane da dire di un solo comma ancora: il settimo, che introduce l'obbligo per i fornitori di tenere un inventario delle violazioni occorse, il quale dia conto delle circostanze in cui si sono verificate, delle conseguenze che ne sono seguite e dei provvedimenti adottati per porvi rimedio. Il comma in esame richiede il costante aggiornamento dell'inventario; sono le Linee Guida, invece, che impongono di utilizzare misure atte a garantire l'integrità e l'immodificabilità delle registrazioni ivi contenute. In assenza di ulteriori precisazioni sul punto, non è dato capire, tuttavia, se l'obbligo in parola presupponga l'impiego della firma digitale e della marca temporale ovvero possa essere assolto anche mediante la periodica esportazione dei *records* su supporti non riscrivibili (come, per esempio, prescritto dal Garante altrove: cfr. le indicazioni fornite in relazione alla figura dell'amministratore di sistema). L'inventario dovrà essere messo a disposizione del Garante qualora l'Autorità ne richieda l'accesso; più efficace, a nostro avviso, sarebbe stato disporre la pubblicazione *on-line* del predetto, sì da permettere agevolmente ad un potenziale "contraente" di un fornitore di servizi TLC di verificare se quest'ultimo abbia, o meno, subito un *data breach*.

Illustrati gli aspetti salienti della disciplina sulla violazione di dati personali, per completezza preme solo accennare che il legislatore, al fine di garantire l'effettività della tutela ivi prevista, ha introdotto nel Codice nuove e specifiche sanzioni amministrative e ha

esteso quella penale contemplata dall'art. 168 all'ipotesi di falsità nelle comunicazioni di cui all'art.32-bis, commi 1 e 8.