CHE FARE IN CASO DI VIOLAZIONI DI DATI PERSONALI: IL GARANTE TRACCIA LA VIA

di Avv. Luca Giacopuzzi[1]

Le brevi note che seguono intendono illustrare al lettore la disciplina di legge delle cd. "violazioni di dati personali" 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. Il tutto alla luce delle indicazioni fornite dal Garante con il **Provvedimento del 4 aprile 2013**, del quale, senza alcuna pretesa di esaustività, viene fornito un primo commento.

Qualunque fatto che mini la sicurezza dei dati personali, se non gestito in modo adeguato, può cagionare all'interessato gravi danni, anche di carattere patrimoniale. Del tutto opportunamente, quindi, il nostro Paese si è dotato di un'organica disciplina in tema di "violazioni di dati personali", che si articola sia in prescrizioni tese a prevenire il rischio di violazioni sia in adempimenti aventi il fine di neutralizzare le conseguenze negative di una violazione già occorsa.

Prima di procedere oltre preme chiarire il significato di "violazione di dati personali", sgombrando il campo da equivoci di sorta. Lo facciamo agevolmente, in quanto il Codice della Privacy precisa che detta locuzione ha ad oggetto 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 i dati trattati nell'ambito dei servizi di comunicazione elettronica), allo stesso tempo è volta a circoscrivere il contesto, oggettivo (i servizi di comunicazione elettronica accessibili al pubblico) e soggettivo (i fornitori dei predetti servizi), nel quale opera la nuova disciplina.

Ciò premesso, e delimitato il perimetro applicativo della fattispecie, osserviamo quanto segue in ordine ai doveri che conseguono ad un episodio di data breach, al dichiarato fine di rispondere al quesito: che fare, in concreto?

CHI - Come già accennato, i nuovi adempimenti gravano unicamente sui fornitori di servizi di comunicazione elettronica accessibili al pubblico e dunque, giusta definizione di legge,

[1]Titolare dello Studio Legale Giacopuzzi – Diritto d'Impresa (www.studiogiacopuzzi.it), e coordinatore del relativo Dipartimento di diritto delle nuove tecnologie.

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); non, invece, coloro che offrono servizi di comunicazione elettronica a gruppi delimitati di individui (si pensi alle aziende che permettono ai dipendenti e ai collaboratori di accedere ad Internet) nè gli esercizi, pubblici o privati, che si limitano a mettere a disposizione dei clienti punti di accesso ad Internet e neppure i gestori dei siti web che diffondono contenuti in rete (cd. content providers).
Il Garante, peraltro, precisa efficacemente che gli obblighi di legge attengono alla particolare natura dei servizi presi in considerazione, di talchè, se la violazione dei dati personali ha ad oggetto una banca dati non strettamente correlata a detti servizi, le prescrizioni non devono essere osservate.
COSA – Il Codice della Privacy dispone che "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". E 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 agli utenti dovrebbe essere dovuta in ogni caso). La considerazione che precede è, tuttavia, probabilmente speciosa perchè il Garante ha chiarito che la predetta comunicazione è da effettuarsi solo nelle situazioni più gravi. Quali? 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. Vanno considerati, infine, gli effetti della violazione, con la conseguenza di ritenere sussistente il pregiudizio per i dati o la riservatezza degli utenti quando dalla violazione può conseguire il furto d'identità, il danno biologico o il danno alla reputazione.
Peraltro, le comunicazioni non sono dovute 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). Ma attenzione: devono essere comunque comunicate agli interessati le violazioni che riguardano le credenziali di autenticazione (binomio username-password), ancorchè dette siano sottoposte ad hashing.

QUANDO – Per espressa disposizione di legge, il fornitore deve comunicare la violazione dei dati personali "senza indebiti ritardi". Da un punto di vista strettamente lessicale la norma non pare immune da censure, poiché "senza indebiti ritardi" è locuzione troppo vaga. Soccorre, ancora, il Garante, disponendo che 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 ipotesi più articolate, la ricognizione dell'evento e l'analisi delle conseguenze sono operazioni che non si esauriscono in tempi brevi, il Provvedimento del 4 aprile 2013 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. La comunicazione ai contraenti e alle altre persone eventualmente interessate, se dovuta, va invece effettuata nel termine di 3 giorni dall'avvenuta conoscenza della violazione.

COME – Né la legge né il Garante prescrivono una specifica modalità cui attenersi per effettuare la comunicazione agli utenti. In sostanza, ciascun fornitore ha piena libertà di decidere quale sia il canale che consente di raggiungere più celermente e con maggior efficacia i soggetti i cui dati sono interessati dalla violazione. Sebbene la comunicazione "one-to-one" sia, all'uopo, da privilegiare, quando il numero dei soggetti è particolarmente elevato non è all'evidenza possibile farvi ricorso. Sono perciò ammesse forme di comunicazione "ad incertam personam", quali, per esempio, la pubblicazione su mezzi di stampa. Infine, i fornitori devono tenere un inventario delle violazioni occorse, il quale dia conto delle circostanze in cui dette si sono verificate, delle conseguenze che ne sono seguite e dei provvedimenti adottati per porvi rimedio. L'inventario dovrà essere messo a disposizione del Garante qualora l'Autorità ne richieda l'accesso; più efficace, a nostro avviso, sarebbe stato prescrivere 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.

PERCHE' – Per etica professionale (segnalare agli utenti le violazioni subite dai propri databases dovrebbe essere un must per gli operatori di telefonia e per gli Internet providers), ma non solo. L'inosservanza dei precetti di cui si è detto è, infatti, severamente sanzionata. L'omessa o ritardata comunicazione al Garante espone ad una sanzione

amministrativa da 25mila a 100mila euro; gravi conseguenze anche per l'omessa o ritardata comunicazione agli utenti, punita con la sanzione amministrativa del pagamento di una somma da 150 a 1000 euro per ciascun contraente o altra persona interessata. La mancata tenuta dell'inventario è, invece, punita con la sanzione da 20 mila a 120mila euro. E ancora. Ove il fornitore, in occasione della comunicazione al Garante, attesti circostanze false, la sanzione è di carattere penale: è prevista la reclusione da 6 mesi a 3 anni, salvo che il fatto costituisca più grave reato.