Data breach: alcune osservazioni sulle linee guida europee

Date : 29 gennaio 2018

Con l'approssimarsi della data in cui sarà applicativo il GDPR ("RGPD" nell'acronimo italiano), va intensificandosi l'elaborazione di linee guida europee. Quelle in materia di *data breach*, tra le più attese, sono state finalmente rese disponibili nell'ottobre 2017 in una prima versione solo in lingua inglese. Nonostante non siano ancora adottate nella stesura definitiva, è prevedibile che non subiranno sostanziali modifiche rispetto al testo già consultabile.

L'occasione è perciò preziosa per alcune riflessioni.

La nozione giuridica di *data breach* e quella corrente

Innanzitutto, va posta una questione concettuale. L'espressione "data breach", infatti, assume in diritto connotazioni ben più estese di quelle correnti soprattutto in contesti strettamente tecnico-informatici. Occorre tenerlo presente.

Il *data breach* giuridico, o "violazione dei dati personali" nella traduzione italiana, include certamente l'attacco a sistemi informatici, l'intrusione o il *data leak*, dunque eventi in cui l'intervento malevolo di terzi è manifesto, ma comprende anche una serie di ipotesi riconducibili all'inosservanza di norme sulla sicurezza da parte del titolare del trattamento.

Anche la mera associazione o confusione indebita di dati personali all'interno della struttura del titolare o l'accessibilità degli stessi a ruoli interni della struttura del titolare non autorizzati costituisce *data breach*.

In definitiva, l'area di ciò che rileva in termini di violazione dei dati personali tende a sovrapporsi e a coincidere con ciò che rileva in termini di osservanza delle misure di sicurezza. Una conseguenza evidente è che ove sia previsto il *data protection impact assessment* (DPIA), ossia la valutazione d'impatto di cui all'art. 35 GDPR, questa dovrà necessariamente coordinarsi (se non proprio integrarsi) anche con gli schemi di reazione e contenimento al *data breach*.

Data breach e continuità operativa

Peraltro – e si tratta di un punto da sottolineare – l'area di ciò che rileva in termini di *data breach* si estende anche oltre la dimensione, strettamente intesa, della sicurezza e include anche ipotesi di significativa alterazione della continuità operativa di un sistema informatico (cfr. pag. 7 linee guida).

Questa è almeno la posizione espressa dal Gruppo di lavoro dei Garanti europei. A pag. 27 viene proposto l'esempio dell'inaccessibilità temporanea di un call center dovuta a un guasto della rete elettrica: «*A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records*».
Tendenzialmente, il concetto di *data breach* viene qui a essere equiparato a quello di rilevante discontinuità nel normale funzionamento di un sistema informatico.

Vale la pena di approfondire la *ratio* di questa posizione, sia perché rende leggermente sfumati i bordi del concetto di violazione dei dati personali (e ciò ha ricadute pratiche) sia perché testualmente l'art. 3.12) GDPR, nel definire questo concetto lo salda al termine «*sicurezza*» e lo sostanzia nella «*distruzione*» o nella «*perdita*», «*modifica*», «*divulgazione*», «*accesso*», ossia in eventi diversi da una mera indisponibilità temporanea dei dati personali.

A ben guardare, tuttavia, l'art. 32 GDPR, espressamente dedicato al profilo della sicurezza, contempla al paragrafo 1, lett. b) anche «*la capacità di assicurare su base permanente… la* disponibilità *e la resilienza dei sistemi e dei servizi di trattamento*». L'interruzione temporanea di un servizio costituisce cioè un *availabilty breach*, ossia una violazione della disponibilità dei dati personali, indipendentemente dal fatto che sia o no permanente.

Data breach: concetto non nuovo, disciplina nuova

Del resto che per *data breach* possa intendersi anche (con la dovuta attenzione alle particolarità di ciascun caso) un *availabilty breach* era stato già chiaramente espresso in passato dal Gruppo di lavoro nell'Opinione 3/2014, che aveva individuato un modello tripartito di violazione dei dati, a seconda che a essere colpita fosse:

1. la confidenzialità delle informazioni (*confidentiality breach*);
2. la loro disponibilità (*availability breach*);
3. la loro integrità (*integrity breach*).

Sono ovviamente ben possibili compromissioni multiple.

È interessante notare la continuità di ragionamento, che le linee guida in commento espressamente rivendicano rispetto all'opinione citata. Si tratta di uno degli esiti di quel faticoso lavoro di rassegna, conservazione e aggiornamento alla luce del Regolamento del glorioso patrimonio di pensiero giuridico elaborato negli anni dai Garanti europei, affinché non sia disperso.

La ragione del precedente giuridico puntualmente confermato è qui del resto chiara: la violazione di dati non costituisce assolutamente un concetto nuovo in materia di protezione dei dati personali, tanto è vero che la definizione contenuta all'art. 4.12) GDPR trova una

corrispondenza pressoché esatta nell'attuale codice privacy (d.lgs. 196/03), all'art. 4.3.g-*bis*), che a sua volta recepisce la definizione di cui all'art. 2.i) dir. 2002/58/CE.

Ciò che è nuovo e costituisce uno dei portati più interessanti del Regolamento è invece la rivoluzionaria estensione della disciplina del *data breach*, che da settoriale (servizi di comunicazione accessibili al pubblico, oltre ad altre ipotesi regolate da fonti diverse) si trasforma (con qualche modifica) in generale, ossia applicabile a tutti i titolari di trattamento indipendentemente dalla tipologia di attività svolta.

Notificazione e comunicazione del *data breach*

La nuova disciplina generale introduce obblighi sinteticamente declinati agli artt. 33 – 34 GDPR, che fissano concisamente requisiti, tempistica, coordinamento con l'Autorità.

È necessario ricordare che non tutti i *data breach* determinano l'obbligo di notificazione al Garante e che non tutti quelli notificati vanno poi comunicati agli interessati (con le evidenti conseguenze, reputazionali e organizzative che la comunicazione comporta).

L'elemento dirimente è costituito dalla valutazione del rischio stimato per i diritti e le libertà degli interessati, quale conseguenza della violazione dei dati personali.

Ove il rischio non sia probabile, il titolare non procederà alla notificazione al Garante e ovviamente neppure alla comunicazione agli interessati. Tuttavia il titolare sarà tenuto a tenere traccia dell'evento (art. 33.5 GDPR) e dell'analisi del rischio svolta su di esso, per futura consultazione e verifica. Viene cioè qui in considerazione un obbligo di *accountability*.

Un esempio concreto di una situazione di questo genere è quello, già proposto, dell'indisponibilità temporanea di dati personali in un call center determinato da un'interruzione della linea elettrica.

Ove il rischio sia invece probabile ma non elevato, il titolare procederà alla notificazione al Garante ma non alla comunicazione agli interessati. Viene qui fatto l'esempio del furto di un cd contenente dati protetti da cifratura (p. 27 linee guida). Ovviamente l'elemento dirimente è la robustezza del sistema di cifratura e la sua tenuta nel tempo.

Ove il rischio sia probabile ed elevato, il titolare procederà tanto alla notificazione al Garante quanto alla comunicazione agli interessati. È per esempio il caso del cliente di una banca che abbia ricevuto l'estratto conto di un diverso cliente della stessa (cfr. p. 28 linee guida).

Casi reali di pronta consultazione

Dall'esperienza recente del Garante italiano per la protezione dei dati personali il giurista può trarre casi di studio assai interessanti per comprendere possibili dinamiche del *data breach* e per orientare l'analisi del rischio. Si veda per esempio la clamorosa e pluriennale vicenda che ha riguardato Telecom Italia s.p.a., affrontata minutamente dal Garante con il provvedimento

6.4.2017 [6376175] n. 176/17 o il più conciso provvedimento nei confronti di Wind Tre s.p.a., GPDP, 11.5.2017 [6431926].

Va solo precisato che i requisiti previsti dalla base giuridica richiamata in questi interventi del Garante è ovviamente quella dell'art. 32-*bis* d.lgs. 196/03 e del provv. GPDP 4.7.2013 [2388260], che è informata a presupposti leggermente diversi da quelli del Regolamento. *Mutatis mutandis* ed evitando automatismi acritici, quelli indicati costituiscono comunque utilissimi precedenti di immediata consultazione.

Da ultimo, non si può non segnalare il recentissimo provvedimento GPDP, 21.12.2017 [7400401]. In esso ovviamente non si fa ricorso alla disciplina generale del *data breach* (il Regolamento non è ancora applicativo), tuttavia sono tratteggiate con grande chiarezza e in anticipo le direttrici lungo le quali si muoverà, e in parte già si muove, l'accertamento del Garante. Due fra tutte: verifica del rispetto del requisito della *privacy by design* e *by default* e dell'utilizzo opportuno della pseudonimizzazione. È qui evidente come il DPIA e in generale il profilo della sicurezza integrino giocoforza la materia del *data breach*.

Il concetto di rischio

Le linee guida forniscono qualche indicazione a proposito della valutazione del rischio, che non si distacca tuttavia molto da quanto già direttamente desumibile dal Regolamento (cfr. anche art. 35). Sotto questo profilo l'interprete rimarrà forse deluso, benché siano forniti comunque criteri ulteriormente elaborabili e sia del resto ben possibile integrare queste considerazioni con quelle contenute, sotto questo specifico profilo, nelle linee guida sul DPIA. In ogni caso, le linee guida oggi in commento forniscono preziosi esempi pratici sull'applicazione dell'analisi del rischio che facilitano certamente l'interprete nella valutazione.

Per un approfondimento della nozione di rischio, il riferimento chiave è ovviamente al considerando 85 GDPR. Qui tra le conseguenze pregiudizievoli in cui si sostanzia il «*rischio per i diritti e le libertà*» degli interessati sono espressamente indicati le seguenti: «***perdita del controllo*** *dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica*».

Preme a chi scrive evidenziare l'espressa indicazione della «*perdita del controllo*» che non figurava *expressis verbis* nel regolamento UE 611/2013. È lecito cogliere in questo richiamo al diritto di controllare i dati personali, che si trova altresì significativamente ribadito al considerando 7 GDPR, un evidente collegamento con quella luminosa tradizione di pensiero che ha approfondito il concetto di *habeas data* e di autodeterminazione informativa, e della quale in Italia si è fatto per decenni lucidissimo interprete il compianto Prof. Stefano Rodotà.

Il diritto alla protezione dei dati personali va cioè correttamente inteso come fondamentale diritto di controllo e decisione riconosciuto all'interessato, diritto rispetto al quale, dunque, i dati personali costituiscono unicamente l'oggetto protetto ma non la *ratio* della tutela. In definitiva chi

guarda solo ai dati personali e crede in tal modo di avere colto il senso della normativa di settore è come il proverbiale uomo che guarda al dito anziché alla luna. Questo va tenuto presente tutte le volte in cui leggiamo che il diritto in commento viene declassato, anche in ben note pronunce di giurisdizione superiore, a una sorta di curioso “totem giuridico” di cui pare arbitrario che il legislatore possa occuparsi.

Ebbene, è confortante (e significativo per l’interprete) prendere atto che il legislatore europeo ha rimarcato che la violazione dei dati personali può ben determinare incisione del fondamentale diritto all’autodeterminazione informativa, che in definitiva il diritto alla protezione dei dati personali è diritto di controllo delle proprie informazioni in un mondo ormai pervasivamente digitale.

Il ruolo del DPO nella valutazione del rischio

Sulla scorta di quanto notato, la valutazione sul rischio è fondamentale e comporta evidentemente responsabilità per qualsiasi sottovalutazione. Essa deve includere non solo un esame della situazione presente e passata ma una proiezione *de futuro*.

Ora, è chiaro che considerati i tempi assai stretti (72 ore dalla conoscenza del *data breach* per la notificazione al Garante), viene a determinarsi una concentrazione di attività critiche, che non può lasciare spazio all’improvvisazione né alla concitazione del momento. Il titolare deve cioè essersi dotato per tempo (*«plan in advance»*, scrivono i Garanti, p. 5) di una procedura chiara e lineare sulla reazione al *data breach*, alla quale affidarsi per un’ordinata gestione dell’emergenza.

Ci si può giustamente chiedere a questo punto quale sia il ruolo del DPO (ove designato) quando l’emergenza effettivamente si verifichi.

Va detto che il legislatore non ha espressamente previsto il coinvolgimento del DPO nella valutazione su un *data breach* in atto e che le stesse linee guida in commento tendono a trascorrere frettolosamente su questo punto (cfr. p. 24 linee guida).

Pare tuttavia a chi scrive che non si possa dubitare della necessità di consultazione del DPO in caso di *data breach*, in applicazione di una serie di ovvie considerazioni sistematiche. In tal senso, è appena il caso di richiamare la *ratio* stessa dell’istituto del DPO, il compito di sorveglianza del rispetto del Regolamento che questa figura assolve ai sensi dell’art. 39.1.b), il generale profilo di consulente giuridico che lo connota, cfr. per esempio art. 39.1.a). Questi inoltre assolve certamente alla funzione di esperto in materia di analisi del rischio, art. 39.1.c), profilo che appare massimamente richiamato proprio nella fase assai critica di valutazione della portata e degli esiti del *data breach*.

Ciò posto, ad avviso di chi scrive, l’art. 33.3.b), che assegna al DPO il ruolo di punto di contatto del titolare nel caso di notificazione del *data breach*, non dovrebbe essere riduttivamente inteso nel senso di postulare un suo coinvolgimento solo successivo e per sole necessità di contatto.

Note conclusive

Le linee guida affrontano direttamente ed evocano implicitamente una serie di altri temi di notevole interesse, che nel breve spazio di questo articolo non possono essere affrontati. Se ne segnala brevemente qualcuno: sanzioni amministrative connesse con il verificarsi del *data breach* e con la tipologia di risposta, competenza dell'Autorità di controllo nel caso di trattamenti transfrontalieri, analisi più dettagliata del rapporto tra DPIA e programmazione della procedura da adottare nel caso di *data breach*, gestione delle revisioni periodiche delle analisi svolte, responsabilità civile del titolare nei confronti degli interessati e del responsabile del trattamento nei confronti del titolare per segnalazioni tardive od omissive.

A cura di: **Enrico Pelino**