filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

Come gestire un Data Breach ai sensi del Nuovo Regolamento UE

04 Settembre 2018
Antonella Di Cerbo

Abstract
Alla luce delle importanti novità introdotte dal Nuovo Regolamento UE 2016/679, il presente articolo mira ad offrire conoscenze utili per identificare e gestire un data breach.
In particolare, sono descritti gli obblighi di *disclosure* previsti a carico del Titolare del trattamento per prevenire, limitare ed i eliminare i danni causati dalla violazione ed i presupposti in presenza dei quali non sono richieste comunicazioni.
In ultimo, al fine di comprendere i risvolti pratici delle nuove disposizioni, si offrono spunti di riflessione in ordine all'applicabilità della nuova disciplina al caso Cambridge Analytica.

Cos'è un data breach e quali sono i rischi più frequenti a cui può dar luogo
Il Regolamento UE 2016/679 dedica una disciplina specifica al "*data breach*", ossia all'ipotesi di **una violazione di sicurezza che comporti accidentalmente, o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque trattati** (Articolo 4 par. 12 RGDP).
Le Linee Guide del Working Party 29 del 3.10.2017 chiariscono che per data breach deve intendersi un **incidente di sicurezza** che può dar luogo: ad una "violazione della confidenzialita?, della disponibilita? ovvero dell'integrita?" dei dati trattati a danno dell'interessato. Si pensi, rispettivamente, ai casi di distribuzione, perdita di accesso ovvero distruzione e modifica accidentali, o non autorizzate, dei dati personali.
Il Considerando 85 del Regolamento Ue indica alcuni tra i principali rischi cui può dar luogo una violazione dei dati personali non affrontata in modo adeguato e tempestivo. In particolare, **tra i rischi più frequenti, vi sono: danni materiali o morali alle persone fisiche, come la perdita del controllo dei dati o la limitazione dei diritti degli interessati; episodi di discriminazione, di furto o usurpazione d'identita?; perdite finanziarie; pregiudizi alla reputazione ovvero di natura economica e sociale a danno dell'interessato**.
Obblighi di *disclosure* e possibili eccezioni
Al fine di porre rimedio alla violazione e di limitare i danni, ai sensi dell'articolo 33 del Regolamento Ue, il Titolare del trattamento, venuto a conoscenza della violazione deve, senza ritardo e, ove possibile, entro 72 ore, notificare l'accaduto all'Autorita? di controllo competente. Trascorso il termine di 72 ore, la notifica deve essere corredata da valide ragioni che giustifichino il ritardo.
La notificazione potrà essere evitata solo laddove sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le liberta? delle persone fisiche. In seguito, se richiesto, sarà onere del titolare del trattamento dimostrare, conformemente al principio di responsabilita?, che le prerogative

dell'interessato non erano suscettibili di subire un pregiudizio.

Esclusa tale ultima eventualità, il titolare deve effettuare la notifica nei modi e nei tempi previsti dal Regolamento. La *ratio* risiede nell'esigenza di offrire all'Autorità di controllo tutta la documentazione utile per le successive verifiche. Pertanto, dovranno essere documentate:

- le circostanze in cui si e? verificata la violazione. In particolare, se possibile, dovranno essere descritte la natura della violazione dei dati personali, le categorie ed il numero approssimativo di registrazioni dei dati in questione;
- il nome e le coordinate di contatto del titolare della protezione dei dati o di altra persona presso cui ottenere informazioni utili;
- le conseguenze della violazione ed i provvedimenti adottati per porvi rimedio ovvero per attenuarne i possibili effetti negativi.

Il mancato rispetto degli obblighi di *disclosure* autorizza il Garante della privacy ad applicare le sanzioni previste dall'articolo 58 comma 2 (vale a dire: avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere i flussi di dati) nonché le sanzioni amministrative di cui all'articolo 83 commi 4 e 5, il cui importo puo? arrivare fino a 10 milioni di euro ovvero al 2% del fatturato totale annuo dell'esercizio precedente.

Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le liberta? delle persone fisiche, il titolare deve altresì darne comunicazione all'interessato in modo chiaro e facilmente comprensibile.

La comunicazione all'interessato è, in ogni caso, esclusa quando il titolare del trattamento utilizzi misure tecniche ed organizzative idonee ad evitare che l'interessato sia esposto a pregiudizi (ad esempio, cifrando le informazioni, quindi rendendo i dati incomprensibili a chiunque non sia autorizzato ad accedervi); ovvero quando abbia adottato, *ex post*, misure atte ad evitare il sopraggiungere di un rischio elevato per i diritti e le liberta? degli interessati. Il titolare può altresì evitare di comunicare all'interessato la violazione laddove ciò richieda sforzi sproporzionati e la conoscenza della stessa possa essere assicurata in egual modo attraverso una comunicazione pubblica o un'altra misura simile.

Laddove il titolare del trattamento, a causa di un'erronea valutazione ovvero dei tempi contingentati, non abbia ancora comunicato all'interessato la violazione dei dati personali, l'Autorita? di controllo, dopo aver valutato la probabilita? che la violazione presenti un rischio elevato, puo? chiedere che vi provveda .

In ogni caso, il Considerando 73 fa salva la possibilità per il diritto dell'Unione o degli Stati membri di imporre limitazioni alla comunicazione di una violazione di dati personali all'interessato, ove cio? sia necessario per la salvaguardia della sicurezza pubblica; per fini connessi alle attivita? di prevenzione, indagine e perseguimento di reati o l'esecuzione di sanzioni penali; per la tutela di altri interessi pubblici dell'Unione o di uno Stato membro, tra cui un interesse economico o finanziario rilevante dell'Unione o di uno Stato membro; per la tenuta di registri pubblici; per ragioni di interesse pubblico generale o, ancora, per la tutela dell'interessato o dei diritti e delle liberta? altrui, compresi la protezione sociale, la sanita? pubblica e gli scopi umanitari.

A seguito della trasmissione della documentazione relativa alla violazione l'Autorità di controllo valuterà le misure idonee a limitare i danni e l'opportunità di comminare una sanzione al titolare del trattamento considerando: la natura, la gravita? e la durata della violazione; l'eventuale dolo; le misure tempestivamente adottate dal titolare per attenuare i danni, il grado di responsabilita? ed eventuali precedenti violazioni pertinenti da parte del titolare.

Per garantire la massima armonizzazione della disciplina nel territorio europeo nonché l'efficacia delle

disposizioni ivi contenute, il legislatore europeo auspica che le Autorita? di controllo dei diversi Stati membri abbiano compiti analoghi e poteri effettivi, tra questi *ex multis*: poteri di indagine; correttivi e sanzionatori; autorizzativi e consultivi.

Considerazioni finali

Alla luce del recente scandalo Cambridge Analytica, è stata evidenziata l'opportunità di estendere il concetto di data breach anche alle ipotesi in cui il titolare non subisca direttamente una violazione, ma sia a conoscenza del trattamento illecito posto in essere dai soggetti terzi a cui ha trasmesso i dati. Il riferimento è al social network Facebook ed all'app *"this is your digital life"* accusata di aver illecitamente creato identikit digitali di più di 50 milioni di utenti.

Infatti è emerso che, anche se il nuovo Regolamento trovasse applicazione nel caso di specie ed in altri analoghi, il titolare del trattamento, venuto a conoscenza della violazione dei diritti degli interessati da parte di un soggetto terzo a cui ha ceduto i dati, non ha l'obbligo di segnalare il data breach.

Pertanto, è auspicabile che la nozione di data breach si riferisca anche alle ipotesi in cui il titolare sia a conoscenza del trattamento illecito posto in essere da terzi ed avente ad oggetto i dati che egli stesso ha trasmesso, soprattutto quando tali violazioni riguardano un elevato numero di interessati ed informazioni sensibili ai sensi dall'articolo 9 del Regolamento UE.

Dal punto di vista giuridico l'obbligo di *disclosure* potrebbe essere esteso al social network argomentando sulla base delle linee guida elaborate dal Working Party 29 ove si fa riferimento alla violazione della confidenzialità come possibile effetto di un incidente di sicurezza, quindi di un data breach. Infatti, la comunicazione non autorizzata dei dati personali agli sviluppatori dell' app. dà luogo ad una violazione di confidenzialita? altamente lesiva per gli interessati, in quanto avente ad oggetto dati relativi alle opinioni politiche, per i quali, tra l'altro, ai sensi del Regolamento, è ammesso il trattamento solo previo consenso espresso ed informato da parte dell'interessato.

TAG: *data breach, GDPR, Regolamento privacy, Trattamento dati personali, Diritto della privacy*