diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

La banca risponde dell’accesso non autorizzato alla banca dati clienti da parte dei dipendenti di un partner commerciale esterno

Autore: Muia' Pier Paolo
In: Giurisprudenza commentata

Garante per la protezione dei dati personali: Ordinanza ingiunzione del 10 giugno 2020 - Registro dei provvedimenti n. 99 del 10 giugno 2020.

Volume consigliato

Il fatto

Nell’estate del 2017 una banca italiana aveva comunicato al Garante di aver riscontrate due episodi di data breach del proprio data base clienti.

In particolare, la banca aveva evidenziato che tra l’aprile 2016 e il luglio 2017 si erano verificate due ipotesi in cui del personale non autorizzato aveva effettuato degli accessi ai dati di oltre settecentomila clienti della banca ed aveva preso visione di numerosi dati personali di questi ultimo, fra i quali: dati anagrafici e di contatto, professione, livello di studio, estremi identificativi di un documento di riconoscimento e informazioni relativi a datore di lavoro, salario, importo del prestito, stato del pagamento, “approssimazione della classificazione creditizia del cliente” e codice Iban.

All’esito del controllo da parte della banca era emerso che i due accessi erano stati effettuati da personale dipendente di una società esterna partner della banca, utilizzando le utenze che erano state loro concesse per l’utilizzo dell’applicativo informatico della banca di gestione del database clienti. In altri termini, **la banca aveva concesso alla società esterna, propria partner commerciale, l’utilizzo dell’applicazione informatica usata dalla banca per gestire la banca dati e alcuni dipendenti di tale società esterna avevano usato le proprie credenziali per prendere visione dei dati di oltre 700.000 clienti della banca rispetto ai quali non aveva autorizzazione all’accesso**.

Diritto & Diritti ISSN 1127-8579

Dopo aver effettuato la propria istruttoria, il Garante per la protezione dei dati personali aveva ritenuto illecito il trattamento dei dati posto in essere dalla banca, configurata quale titolare del trattamento stesso, in quanto era stato effettuato in violazione delle misure di sicurezza minime previste dal codice privacy e dal relativo disciplinare tecnico.

In particolare, secondo il Garante la violazione era consistita nel fatto che la banca non aveva adottato un idoneo sistema di autorizzazione per l'accesso e l'utilizzo dell'applicativo informatico e per il fatto che tale non fossero previsti dei limiti di accesso che circoscrivessero ai vari profili autorizzati all'accesso la visibilità e consultabilità dei soli dati necessari per compiere le operazioni per cui erano autorizzati ad accedere ai dati stessi. In altri termini, **l'applicativo informatico usato dalla banca avrebbe dovuto, da un lato, prevedere un sistema di autorizzazione all'accesso idoneo ad impedire l'accesso al sistema da parte di qualunque dipendente della società esterna e, dall'altro lato, prevedere un sistema che permetteva ai soggetti autorizzati all'accesso di consultare soltanto i dati che sarebbero loro serviti per svolgere l'attività per la quale avevano ricevuto l'autorizzazione ad accedere all'applicativo.**

In secondo luogo, secondo il Garante, la violazione della banca era consistita altresì nel fatto che il sistema di conservazione del log di tracciamento degli accessi nell'applicativo informatico era inadeguato e non erano previsti dei sistemi di alert che segnalassero il compimento di operazioni attraverso detto applicativo.

Le difese della banca

A fronte di dette contestazioni, la banca ha svolto le proprie difese sostenendo che il sistema di autorizzazione per l'accesso all'applicativo informatico era conforme alle norme in materia di privacy vigenti all'epoca dei fatti e che nel caso di specie non si era verificato alcun accesso abusivo al sistema (cioè di soggetti non autorizzati all'accesso), ma si era verificato un accesso indebito da parte di personale autorizzato della società esterna che aveva sfruttato un bug del sistema per prendere visione di dati che non riguardavano pratiche in loro gestione.

In secondo luogo, la banca rilevava come la stessa avesse correttamente definito anche i criteri di profondità degli accessi, avendo definito preventivamente all'inizio del trattamento quali dati ogni soggetto autorizzato a accedere all'applicativo avrebbe potuto consultare e cioè i soli dati necessari per svolgere le operazioni e l'attività per cui aveva ottenuto l'accesso. Mentre nel caso di specie, l'accesso a dati ulteriori da parte del personale della società esterna era avvenuto perché detto personale aveva sfruttato una falla informatica nell'applicativo e aveva così eluso le restrizioni di visibilità dei dati.

Diritto & Diritti ISSN 1127-8579

Infine, per quanto riguarda i log di tracciamento, la banca rilevava come il fatto che gli stessi non contenessero alcuni dati relativi agli accessi non rendeva il sistema di log totalmente inadeguato; mentre, rispetto alla adozione degli alert, la banca evidenziava come sussistesse un sistema di firewall che al superamento di un certo traffico elevato, inviava degli alert, ma che nel caso di specie tali segnalazioni non erano state effettuate dal firewall perché il numero di accessi effettuati era in linea con il normale uso dell'applicativo ad parte della banca e assolutamente non anomalo.

In conclusione la banca chiedeva l'archiviazione del procedimento sanzionatorio in considerazione di tutte le proprie difese e soprattutto in considerazione del fatto che gli interessati non avessero subito alcun pregiudizio in conseguenza degli accessi ai propri dati.

Il parere del Garante

Il Garante ha preliminarmente evidenziato che, nonostante l'eventuale mancanza di pregiudizi a carico degli interessati, l'intervento del Garante è comunque necessario stante l'illeicità del trattamento dovuta alla inadeguatezza delle misure di sicurezza e stante la necessità di salvaguardare i diritti e le libertà degli interessati coinvolti nel data breach.

L'autorità di controllo ha ritenuto che le difese della banca non fossero idonee ad escludere la responsabilità di quest'ultima in considerazione del fatto che dall'istruttoria è emerso che **l'Impostazione dei sistemi di autorizzazione per l'accesso all'applicativo informatico erano non in linea con la normativa in materia di protezione die dati personali, i quali risultavano deboli e progettati in maniera non corretta: tant'è che il sistema di segregazione dei dati non era stato in grado di impedire ai dipendenti della società partner di prendere visione dei dati rispetto ai quali non erano autorizzati ad accedere**. Infatti, nonostante le misure di sicurezza adottate, del personale ignoto della società partner della banca aveva utilizzato le credenziali che erano state loro assegnate dalla banca e avevano preso visione di dati che non rientravano nelle pratiche che erano state assegnate alla società partner.

Secondo il Garante, quindi, **tali debolezze dell'applicativo informatico utilizzato dalla banca sono responsabilità della banca stessa, in quanto titolare del trattamento, e pertanto la stessa deve rispondere per non avere garantito l'efficacia del sistema**.

Nel caso in cui i profili di autorizzazione fossero stati correttamente impostati e configurati con le limitazioni di accesso, ciascun operatore della società partner esterna avrebbe potuto consultare solo i dati relativi alle pratiche di propria competenza, in quanto il sistema di autorizzazione avrebbe bloccato ogni accesso su pratiche gestite da altri soggetti. Soltanto in tal caso, i sistemi di sicurezza sarebbero stati adeguati: in mancanza di ciò, la banca è responsabile del fatto che detti soggetti abbiano avuto la possibilità di visionare anche pratiche non di propria competenza.

Diritto & Diritti ISSN 1127-8579

In conclusione, il Garante, tenuto conto della gravità del pericolo e del pregiudizio derivati dal data breach nonché dal comportamento tenuto dalla banca, ha sanzionato quest'ultima con il pagamento di un importo pari a Euro 600.000.

Volume consigliato

https://www.diritto.it/la-banca-risponde-dellaccesso-non-autorizzato-alla-banca-dati-clienti-da-parte-dei-dipendenti-di-un-partner-commerciale-esterno/

Diritto & Diritti ISSN 1127-8579