DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Il Piano Ispettivo del Garante Privacy: impatti per le banche

6 Aprile 2023

Luca Tufarelli, Partner & Founder, Ristuccia Tufarelli & Partners
Maria Lilia La Porta, Senior Associate, Ristuccia Tufarelli & Partners

DB non solo diritto bancario

Luca Tufarelli, Partner & Founder, Ristuccia Tufarelli & Partners

Maria Lilia La Porta, Senior Associate, Ristuccia Tufarelli & Partners

Luca Tufarelli

L'avvocato Luca Tufarelli, Partner e socio fondatore dello studio Ristuccia Tufarelli & Partners, ha conoscenze specifiche nei campi del diritto civile, commerciale, amministrativo e del diritto dell'informatica dove assiste sia soggetti privati che pubblici. Ha contribuito alla realizzazione di progetti speciali nei settori delle tecnologie innovative, delle telecomunicazioni, della informatizzazione della PA e del commercio elettronico occupandosi anche degli aspetti consumeristici e di compliance regolamentare (privacy, tutela del mercato e vigilanza delle comunicazioni).

Studio associato

Ristuccia Tufarelli & Partners

1. Premessa – Il Piano Ispettivo 2023

Il presente contributo è volto ad esaminare i punti di interesse per l'attività ispettiva del Garante per la protezione dei dati personali ("Garante") con particolare riferimento al settore bancario.

Il Garante, con il Provvedimento n. 23 del 26 gennaio 2023, ha deliberato e pianificato l'attività ispettiva per il periodo da gennaio a giugno 2023.[1]

La pubblicazione del Piano ispettivo ha la finalità di rendere note ai titolari del trattamento le tematiche che saranno principale oggetto dei controlli effettuati dal Garante anche mediante l'ausilio del Nucleo Speciale Tutela della Privacy e Frodi Tecnologiche della Guardia di Finanza. In particolare, il Garante ha dichiarato che verranno condotti almeno 60 accertamenti ispettivi, che potranno essere svolti anche mediante verifiche online. Resta inteso che gli accertamenti possono essere in ogni caso promossi da reclami o segnalazioni o derivare dalla rilevazione di criticità in sede di controlli online.

Il Piano ispettivo prevede innanzitutto una continuità rispetto al Piano 2022, in quanto è pianificato, in via prioritaria, il completamento delle attività ispettive già iniziate nel corso del secondo semestre dell'anno 2022. Le principali aree che sono state individuate per condurre le ispezioni sono:

a) *verifiche sui gestori dell'identità digitale e sui fornitori di servizi che utilizzano SPID e CIE (anche ad uso professionale o per minori) nell'ambito di servizi online offerti anche mediante APP da parte delle pubbliche amministrazioni;*

b) *verifiche in ordine alla corretta implementazione delle Linee guida sui cookie e gli altri strumenti di tracciamento anche attraverso lo strumento degli accertamenti online;*

c) *prosecuzione delle verifiche in materia di trattamento di dati personali attraverso attività di tele-marketing e tessere di fidelizzazione.*

Saranno svolti, inoltre, "*altri accertamenti nei confronti di soggetti pubblici e privati, al fine di verificare*

1 Garante per la protezione dei dati personali, Provvedimento n. 23 del 26 gennaio 2023, doc web n. 9862660 *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9862660*

l'osservanza delle disposizioni in materia di protezione dei dati personali, ivi incluse le istruttorie relative a reclami e segnalazioni formali proposti all'Autorità ed in istruttoria presso i relativi Dipartimenti e Servizi".

Alla luce delle macro aeree indicate, stante l'interesse generale alla compliance in materia di protezione dei dati personali, è possibile ritenere che i titolari maggiormente esposti al rischio dell'accertamento ispettivo del Garante sono coloro che effettuano operazioni di trattamento (i) quali gestori di identità digitale e fornitori di servizi SPID e CIE, (ii) mediante l'utilizzo di cookie e (iii) attraverso attività di telemarketing e fidelity card.

I settori indicati sono tutt'oggi di particolare interesse per il Garante, in quanto è di recente pubblicazione (i) il provvedimento del Garante con il quale è stato approvato il Codice di condotta per le attività di telemarketing e teleselling del 09 marzo 2023,[2] nonché (ii) il Report della Task Force dell'EDPB (European Data protection Board) sui banner cookie del 17 gennaio 2023[3].

Il suggerimento per tutti i titolari del trattamento è, qualora non sia già stato fatto, di effettuare una attenta analisi della loro presenza *on line* verificando: (i) la conformità dei loro siti e dei processi di interazione con gli utenti alle prescrizioni della normativa in materia di protezione dei dati personali ed in particolare delle richiamate novità introdotte dalle recenti Linee Guida e Provvedimenti del Garante nazionale ed europeo (ii) l'adozione di tutte le misure necessarie per garantire sin dalla progettazione la tutela dei trattamenti dei dati personali e delle libertà e dei diritti degli interessati.

2. La banca *data driven* e l'approccio basato sul rischio

L'attività ispettiva del Garante in generale e in particolare con riferimento alle aree indicate nel Piano ispettivo per il primo semestre 2023 interessa il settore bancario proprio in quanto le banche hanno ormai reso centrale il dato e operano secondo il principio del *data driven banking*.

2 Garante per la protezione dei dati personali, "*Provvedimento di approvazione del codice di condotta per le attività di telemarketing e teleselling presentato dalle associazioni promotrici - 9 marzo 2023*", Provvedimento n. 70 del 9 marzo 2023, doc web n. 9868813, *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9868813*

3 EDPB *https://edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-cookie-banner-taskforce_en*

Per *data driven banking* si intende l'insieme delle attività che sfruttano i dati dei clienti e dei lead acquisiti on line per fornire una pluralità di servizi bancari, spesso offerti dalla banca ai propri clienti anche mediante piattaforme e servizi di fornitori terzi.

In tale contesto, le banche hanno dovuto e devono necessariamente effettuare le operazioni di trattamento legate alle attività e ai servizi digitali offerti prestando la massima attenzione alla protezione dei dati personali dei clienti implementando altresì sin dalla progettazione misure di sicurezza (sia tecniche che organizzative) che possano ridurre al minimo il rischio per i diritti e le libertà degli interessati.

Risulta perciò di fondamentate importanza che le banche adottino un approccio basato sul rischio (*risk based approach* – "RBA") che ponga sin dalla progettazione l'attenzione tanto alla data security che alla data protection. Per RBA si intende l'analisi preventiva del contesto del trattamento, del grado di probabilità e di gravità dei potenziali rischi ai quali potrebbe essere esposto l'interessato predisponendo nel contempo un piano di azione volto a limitare o mitigare il verificarsi del rischio stimato.

La valutazione del rischio potrà essere differente a seconda che si tratti di una banca d'affari, di una banca di credito cooperativo, di una banca popolare o di una banca virtuale, in quanto potranno essere diversi i servizi digitali offerti e/o la strategia di marketing scelta. Ciascuna per i prodotti e servizi implementati potrà essere soggetta ai controlli ispettivi del Garante proprio con riferimento alle macroaree indicate nel Piano Ispettivo per il primo semestre 2023, in quanto la maggioranza delle banche opera on line attraverso (i) siti web e applicazioni mobili (App), (ii) strutture di marketing e di direct marketing che offrono ai clienti servizi bancari e finanziari diretti e/o per il tramite di piattaforme terze dedicate e (iii) strumenti di fidelizzazione della clientela e/o dei lead acquisiti (i.e. telemarketing, fidelity card, premi e payback, etc. etc.).

L'esposizione su internet, in particolare, consente agli ispettori del Garante o alla Guardia di finanza di effettuare un controllo mediante consultazione diretta dei siti web o App. Tale controllo interessa in particolar modo la compliance legata alla disciplina dei cookie. Pertanto, una particolare attenzione deve essere dedicata alla conformità dei siti web, app e piattaforme informatiche utilizzate, che devono essere costantemente monitorate anche sotto il profilo della sicurezza e in funzione all'utilizzo dei cookie.

vedi l'articolo online

Allo stesso tempo, le banche non devono sottovalutare il rischio connesso al trattamento per finalità di direct marketing dei dati personali raccolti che, si ricorda, proprio con riferimento ai c.d. indirizzi elettronici (mail, telefono, wup, etc. etc.) necessita del consenso dell'interessato e deve rispettare regole ben precise.

Le suddette attività di trattamento devono essere oggi più che mai attenzionate dalle banche per evitare di incorrere in sanzioni in caso di verifica ispettiva nella quale vengano riscontrate criticità o trattamenti illegittimi. Al contempo, non deve essere sottovalutato o ritenuto meno rilevante ogni aspetto legato alla data protection e alla data security. Le operazioni di trattamento devono essere ispirate al suddetto principio RBA e devono essere costantemente monitorate, anche mediante assessment periodici, in modo da rendere il gap di criticità tendente allo zero.

A tal proposito, devono essere considerate - e mai sottovalutate - tanto le misure di sicurezza organizzative, quanto le misure tecniche che ovviamente attengono maggiormente alla sicurezza informatica, quindi alla sicurezza delle reti e dei sistemi, alla conservazione dei dati, ai sistemi di autenticazione e a tutte le misure implementate al fine di mitigare il rischio connesso al trattamento.

L'operazione di scelta ed adozione delle misure di sicurezza deriva da una corretta implementazione del principio del RBA nello svolgimento della valutazione del rischio legato al trattamento ed alle libertà e diritti degli interessati, in quanto è dall'esito della valutazione del rischio che vengono individuate le misure di sicurezza adeguate che devono essere adottate.

Con riferimento al settore bancario, è possibile individuare quattro tipologie principali di rischio, che devono dunque essere sottoposte a maggiori controlli. Devono essere ben individuati e stimati i rischi connessi (i) alla tipologia di dati trattati, consistenti principalmente in dati bancari, definiti dal Garante quali "*dati di particolare delicatezza*"; (ii) agli strumenti e sistemi mediante i quali viene effettuato il trattamento, tra i quali ad esempio le APP e i servizi di home banking; (iii) all'errore umano o all'azione di un malintenzionato; (iv) al contesto e alla sicurezza fisica del trattamento.

3. Provvedimenti sanzionatori in materia bancaria

Il Garante Privacy ha emanato di recente diversi provvedimenti sanzionatori nei confronti di alcune banche, in seguito ad accertamenti dai quali è emerso un trattamento illegittimo dei dati e nelle cui motivazioni il Garante ha espresso il carattere particolarmente delicato dei dati bancari quale elemento preso in considerazione, ai sensi dell'art. 83 par. 2 del GDPR, ai fini dell'applicazione della sanzione amministrativa pecuniaria e della relativa quantificazione.

Il primo provvedimento attiene ad una criticità legata alle misure di sicurezza organizzative. Si tratta del Provvedimento n. 202 del 26 maggio 2022[4], con il quale il Garante ha comminato alla banca una sanzione amministrativa pecuniaria di € 100.000,00 per la violazione del principio di liceità, correttezza e trasparenza e del principio di integrità e riservatezza per aver comunicato - per carenza di istruzioni al personale - a un terzo non autorizzato i dati legati al conto corrente dell'interessato reclamante.

Il Garante nel determinare l'ammontare della sanzione ha tenuto conto del fatto che l'istituto bancario fosse stato già in passato destinatario di un provvedimento analogo[5], sintomo che il titolare non abbia adottato nel frattempo misure adeguate ad evitare l'accadimento del medesimo rischio.

Sempre nei confronti della stessa banca il Garante con il Provvedimento n. 272 del 28 luglio 2022[6] ha accertato una violazione del principio di integrità e riservatezza, della sicurezza del trattamento e del principio di privacy by design causata da accessi illeciti alle posizioni contabili della reclamante da parte di un dipendente. L'istituto bancario non aveva implementato idonei alert atti ad individuare comportamenti anomali o a rischio relativi alle operazioni di inquiry eseguite dal personale. Si tratta di un provvedimento legato alla carenza di misure di sicurezza organizzative, analogo ad altro provvedimento[7] già emanato nei confronti del medesimo istituto bancario, per cui il Garante ha affermato che "*il ripetersi di queste violazioni mette in evidenza la necessità di un supplemento di riflessione, da parte del titolare del trattamento, rispetto all'adeguatezza delle procedure volte a verificare il corretto assolvimen-*

4 Garante per la protezione dei dati personali, Provvedimento n. 202 del 26 maggio 2022, doc web 9784626.
5 Garante per la protezione dei dati personali, Provvedimento n. 438 del 16 dicembre 2021, doc web 9742468.
6 Garante per la protezione dei dati personali, Provvedimento n. 272 del 28 luglio 2022, doc web 9812423.
7 Garante per la protezione dei dati personali, Provvedimento n. 270 del 27 maggio 2021, doc web 9718112.

vedi l'articolo online

to delle istruzioni da parte delle persone designate al trattamento dei dati".

Infine, il Provvedimento n. 4 del 14 gennaio 2021[8], ha ad oggetto criticità legate alla sicurezza del trattamento effettuato da due banche e in particolare la sanzione è stata comminata per un "utilizzo improprio di un'utenza tecnica" non rilevato dai sistemi di controllo. Si tratta di una violazione legata alla mancata adozione di misure tecniche e organizzative atte a garantire un livello di sicurezza adeguato al rischio, determinata dalla carenza di un generale approccio basato sul rischio e dall'assenza di una procedura di valutazione del rischio. Su queste basi, il Garante ha comminato una sanzione amministrativa pecuniaria per una somma pari allo 0,1% dei proventi conseguiti dalle due banche con riferimento al bilancio d'esercizio per l'anno 2019, corrispondente rispettivamente a € 1.650.210,00 ed a € 315.023,00.

*****

In conclusione, la particolare delicatezza attribuita dal Garante al dato bancario e il principio del data driven banking, impongono alle banche di agire secondo un approccio basato sul rischio in modo da poter adottare misure di sicurezza sia tecniche che organizzative adeguate a eliminare o mitigare i rischi connessi ai trattamenti. Alla base di tale approccio occorre porre una attenta valutazione dei rischi e l'effettuazione di adeguate valutazioni di impatto di tali trattamenti sulle libertà e sui diritti fondamentali degli interessati. Questo al fine di garantire la sicurezza e la protezione dei dati nonché la tutela degli interessati e, in caso di accertamento, scongiurare l'ipotesi di essere sottoposti ad un provvedimento sanzionatorio per violazione della normativa di settore.

8 Garante per la protezione dei dati personali, Provvedimento n. 4 del 14 gennaio 2021, doc web 9582744.

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it