Garante per la protezione
dei dati personali

Dati bancari: accesso non autorizzato e misure di sicurezza

PROVVEDIMENTO DEL 23 LUGLIO 2009

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

IN DATA ODIERNA, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Giuseppe Fortunato e del dott. Mauro Paissan, componenti, e del dott. Filippo Patroni Griffi, segretario generale;

VISTO il d.lg. 30 giugno 2003, n. 196 (*Codice in materia di protezione dei dati personali*);

VISTA la segnalazione presentata da XY nei confronti di SanPaolo Banco di Napoli S.p.A. in ordine a una comunicazione a terzi di dati bancari relativi all'interessata, successivamente utilizzati nell'ambito di un procedimento di pignoramento presso terzi;

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il dott. Giuseppe Fortunato;

PREMESSO

1. Con segnalazione pervenuta in data 11 aprile 2007, è stato rappresentato che XY, già titolare di un conto corrente presso *"l'agenzia di Pomigliano D'Arco del Sanpaolo Banco di Napoli S.p.A."*, in data 13 luglio 2006 ne apriva uno nuovo (risultato cointestato con la figlia) presso altra agenzia del medesimo istituto di credito (quella di Napoli-Chiaiano), che provvedeva anche a curare l'estinzione del rapporto preesistente (v. p. 1 della segnalazione).

In data 21 marzo 2007 veniva notificato alla segnalante un pignoramento presso terzi sul nuovo conto corrente. Non potendo, a detta della segnalante, il creditore oppignorante essere a conoscenza dell'esistenza del nuovo conto corrente, tale informazione sarebbe stata frutto di *"una violazione della privacy da parte degli addetti alla filiale di Pomigliano D'Arco del San Paolo Banco di Napoli S.p.A., unici che hanno potuto fornire* [al creditore] *le notizie di cui si è avvalso per la notificazione del precisato atto"* (cfr. segnalazione cit.).

2. Nell'ambito di controlli ispettivi disposti dall'Autorità nei confronti delle banche appartenenti al gruppo Intesa SanPaolo ed effettuati presso la capogruppo, al fine di verificare (tra l'altro) gli accessi che hanno interessato il menzionato conto corrente, è emerso che *"ad oggi la struttura in relazione all'organizzazione dei sistemi informativi è divisa prevalentemente in due macroaree denominate "sistema target" e "sistema cedente". Il primo deriva dai sistemi informativi ereditati dal gruppo SanPaolo e è quello che, a regime (in gran parte entro il 2008), ingloberà tutti i sistemi dei diversi istituti confluiti nel gruppo. Il secondo è quello di matrice Intesa, in corso, che, attraverso un'articolata procedura di migrazione, gradualmente sta confluendo nel "sistema target"*. Banco di Napoli S.p.A., peraltro, fa parte del sistema *target* (*cfr.* verbale operazioni compiute del 22 maggio 2008, p. 2) a far data dal 2000 (*v.* presentazione del Gruppo Intesa SanPaolo, agg. 1° aprile 2009 sul sito internet della banca).

Con specifico riferimento al caso di specie, nel corso degli accertamenti ispettivi sono risultati

(*v.* nota Intesa SanPaolo S.p.A. Direzione Internal Auditing del 29 maggio 2008) effettuati accessi indebiti, compiuti da un terminale posto presso la filiale di Pomigliano D'Arco, agenzia presso la quale il conto corrente era già stato estinto. In particolare, tali accessi, relativi all'*"esposizione movimenti da data e saldo"* (del 26 febbraio 2007 e 12 marzo 2007), sono stati effettuati immotivatamente con le credenziali del direttore pro-tempore della filiale, che risulta *"collocato a riposo a far data dal 31 dicembre 2007"*(*cfr.* verbale di operazioni compiute del 29 maggio 2008, p. 2).

Gli accertamenti hanno altresì permesso di appurare che tali accessi sono stati effettuati da un terminale *"che consente l'interoperabilità tra filiali della stessa area geografica (nella fattispecie Napoli e provincia)"*; tale interoperabilità *"di norma è assegnata esclusivamente all'unità organizzativa di area territoriale"* e non alle filiali come quella di Pomigliano d'Arco. Rispetto alla rilevata anomalia i rappresentanti della banca hanno dichiarato essere stati intrapresi *"ulteriori accertamenti in ordine alle cause dell'errata configurazione del terminale"* (*cfr.* verbale di operazioni compiute del 29 maggio 2008, p. 2).

3. Alla luce di quanto esposto, risulta che presso Banco di Napoli S.p.A. è stato effettuato, in assenza di consenso dell'interessata o di altro legittimo presupposto, un trattamento illecito di dati riferiti alla segnalante (artt. 11, lett. *a*), 23 e 24 del Codice), nelle forme della consultazione effettuata, in tre distinte circostanze (in data 26 febbraio e 12 marzo 2007) mediante le credenziali di autenticazione dell'allora direttore di filiale, discostandosi dalle istruzioni impartite (artt. 4, comma 1, lett. *h*), 30, 167 e 169 del Codice).

Tale trattamento illecito è peraltro stato possibile, nelle forme in cui è avvenuto, anche grazie all'utilizzo di una postazione erroneamente configurata (che consentiva la visualizzazione anche a livello di filiale di informazioni relative alla clientela prevista per i terminali utilizzati presso unità organizzative di *"area territoriale"*), tenuto conto del modello tecnico-organizzativo interno predisposto dalla banca: ciò in violazione degli artt. 3 e 31 ss. del Codice, norme che prescrivono misure (organizzative e di sicurezza) finalizzate alla riduzione di accessi non autorizzati o non conformi alle finalità del trattamento.

Impregiudicati gli eventuali profili di responsabilità civile (art. 15 del Codice) e le eventuali violazioni penalmente rilevanti per cui si dispone la trasmissione degli atti alla Procura competente, va rilevato che Banco di Napoli S.p.A. ha adottato le misure di sicurezza *"minime"* a protezione dei dati dei clienti trattati con l'ausilio di strumenti elettronici conformi a quanto prescritto dagli artt. 33 e 34 del Codice e dalle regole 1-26 dell'Allegato B) al Codice.

Deve tuttavia prescriversi alla banca di adottare idonee misure organizzative e, ai sensi dell'art. 31 del Codice, di sicurezza, tese sia a garantire la scrupolosa vigilanza sull'operato degli incaricati, sia a sensibilizzare gli incaricati al rispetto delle istruzioni ricevute anche nel corso delle iniziative formative (prescritte dalla regola 19.6 dell'Allegato B) al Codice).

TUTTO CIÒ PREMESSO, IL GARANTE

1. ritenuto illecito il trattamento di dati personali effettuato presso Banco di Napoli S.p.A. da un proprio incaricato (punto 3), ai sensi dell'art. 154, comma 1, lett. *c*), del Codice, prescrive a Banco di Napoli S.p.A. di adottare, immediatamente e comunque non oltre il 30 settembre 2009, idonee misure organizzative e idonee misure di sicurezza tese sia a garantire la scrupolosa vigilanza sull'operato degli incaricati, sia a sensibilizzare gli stessi incaricati al rispetto delle istruzioni ricevute in occasione di iniziative formative (prescritte dalla regola 19.6 dell'Allegato B) al Codice) (punto 3);

2. richiede, ai sensi dell'art. 157 del Codice, a Banco di Napoli S.p.A. di comunicare a questa

Autorità, entro e non oltre il 15 ottobre 2009, le misure adottate per dare attuazione alle prescrizioni indicate al punto 1 del presente dispositivo;

3. dispone la trasmissione degli atti e di copia del presente provvedimento all'autorità giudiziaria per le valutazioni di competenza in ordine agli illeciti penali che riterrà eventualmente configurabili.

Roma, 23 luglio 2009

Il presidente
Pizzetti
Il relatore
Fortunato
Il segretario generale
Patroni Griffi