LaScala

STUDIO LEGALE E TRIBUTARIO
in association with
FIELD FISHER WATERHOUSE

Focus on

Le nuove prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie

Giugno 2011

www.iusletter.com

Le "*Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie*", contenute nel recente provvedimento del Garante della Privacy in data 12 maggio 2011 (pubblicato sulla Gazzetta Ufficiale in data 3 giugno 2011), introducono importanti novità nel delicato settore della gestione dei sistemi informativi bancari.

L'Autorità è intervenuta a seguito di ripetute segnalazioni da parte di clienti di istituti di credito aventi ad oggetto l'indebita comunicazione a soggetti terzi, verosimilmente da parte di dipendenti, di informazioni bancarie relative alla clientela, per scopi del tutto estranei alle finalità della banca (in particolare, nell'ambito di giudizi relativi a separazioni personali tra coniugi e procedure esecutive).

Il Garante ha, quindi, prescritto l'adozione di nuove e più stringenti misure di sicurezza, in alcuni casi qualificate come "necessarie", in altri semplicemente come "opportune", finalizzate ad attuare un sistema di controlli nella gestione dei dati personali che consenta di prevenire il ripetersi di episodi analoghi. Misure la cui adozione potrà determinare un impatto significativo nella gestione dei sistemi informativi bancari, sia sotto il profilo dell'organizzazione dei processi aziendali, sia sotto il profilo delle dotazioni tecnologiche.

A seguito di un'accurata istruttoria condotta dal Garante, di concerto con l'Associazione Bancaria Italiana (ABI), la circolazione delle informazioni riferite alla clientela nell'ambito di un gruppo bancario è stata scomposta in tre distinte categorie: *(i)* comunicazioni di dati personali tra banche appartenenti al medesimo gruppo; *(ii)* circolazione dei dati tra agenzie o filiali della stessa banca; *(iii)* circolazione dei dati nell'ambito della stessa agenzia o filiale.

In proposito, è emerso che le banche, anche facenti parte di un medesimo gruppo, generalmente agiscono quali autonomi titolari del trattamento, con la conseguenza che i flussi di dati personali riferiti ai clienti nell'ambito dei gruppi bancari si configurano come comunicazione a terzi.

Il Garante ha, quindi, subordinato i flussi infragruppo *(i)* ad una previa informativa – attraverso cui la clientela venga debitamente informata (ai sensi dell'art. 13

Codice della Privacy, di seguito "CP") del fatto che i dati personali ad essa relativi potranno essere oggetto di comunicazione ad altre società nell'ambito del medesimo gruppo bancario, le quali opereranno in qualità di autonomi titolari del trattamento – e, ove non ricorra un'ipotesi di esenzione (art.24 CP), all'acquisizione del consenso informato dell'interessato (art. 23 CP).

Resta, naturalmente, esclusa da tale ambito la circolazione dei dati tra diverse agenzie o filiali di una medesima banca, che, svolgendosi entro la sfera di controllo di un'unica banca titolare di trattamento, non costituisce un'operazione di comunicazione a soggetti terzi.

L'Autorità ha, poi, prescritto agli operatori del settore alcune misure ritenute necessarie, alle quali gli istituti di credito saranno tenuti ad adeguarsi entro 30 mesi a partire dal 3 giugno 2011 (data di pubblicazione sulla Gazzetta Ufficiale del provvedimento).

Tali prescrizioni riguardano innanzitutto la gestione dei sistemi informativi contenenti i dati relativi alla clientela; attività spesso esternalizzata a società terze o a società di servizi facenti parte del gruppo bancario.

Il Garante ha ritenuto opportuno formulare alcune prescrizioni in merito alle modalità con le quali la banca o il gruppo bancario possano garantire la trasmissione dei dati personali relativi ai clienti all'*outsourcer* che gestisce i sistemi informativi, evidenziando come l'eventuale qualificazione delle citate società di gestione dei sistemi informativi quali autonomi "titolari del trattamento" potrà avere luogo solo in presenza di particolari condizioni. L'Autorità ha, infatti, registrato numerosi casi in cui tali società (talvolta appartenenti allo stesso gruppo) sono qualificate come autonome titolari del trattamento senza che ve ne siano i presupposti. Pertanto l'Autorità ha precisato che la qualifica di "titolare del trattamento" non potrà essere attribuita all'*outsourcer* e sarà ascrivibile solamente alla banca nei casi in cui questa mantenga l'effettivo potere di *(i)* assumere decisioni relative alle finalità del trattamento, *(ii)* impartire istruzioni e direttive vincolanti nei confronti delle società di gestione dei sistemi informativi e *(iii)* svolgere funzioni di controllo rispetto all'operato delle medesime e degli incaricati delle stesse.

Ne consegue che ogniqualvolta il trattamento dei dati personali dei clienti da parte della società di gestione dei sistemi informativi sia svolto, come spesso accade, senza che tali poteri decisionali risultino posti effettivamente in capo alla società *outsourcer* , le banche dovranno essere considerate gli unici "titolari del trattamento" e le società operanti in *outsourcing* dovranno essere designate quali "responsabili" (ai sensi degli artt. 4, comma 1, lett. g) e 29, commi 4 e 5, CP).

Estremamente rilevanti sono, poi, le **misure prescritte dal Garante per la tracciabilità delle operazioni di accesso ai dati, anche solo per finalità di consultazione, poste in essere dai dipendenti delle banche**. Il provvedimento ha stabilito in proposito che le banche dovranno adottare idonee soluzioni informatiche al fine di assicurare il controllo delle attività svolte sui dati dei clienti e dei potenziali clienti da ciascun incaricato del trattamento.

L'Autorità ha stabilito, infatti, che dovranno essere adottate idonee soluzioni informatiche che permettano un efficace controllo dei trattamenti condotti sui dati presenti nei diversi database utilizzati dalla banca (ai sensi dell'art. 31 CP). Tali misure comprendono la registrazione dettagliata (in un apposito *file* di *log*) delle informazioni riferite alle operazioni effettuate sui dati bancari. Così, per ogni operazione di accesso ai dati bancari effettuata da un incaricato del trattamento, i *file* di *log* dovranno tracciare almeno le seguenti informazioni:

- codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso;
- data e ora di esecuzione;
- codice della postazione di lavoro utilizzata;
- codice del cliente interessato dall'operazione di accesso ai dati bancari da parte dell'incaricato;
- tipologia del rapporto contrattuale del cliente a cui si riferisce l'operazione effettuata (es. numero del conto corrente, fido (mutuo, deposito titoli).

Tali misure, che comportano un'attività di monitoraggio dei dipendenti della banca, dovranno peraltro essere adottate in osservanza della vigente disciplina in mate-

ria di controllo a distanza dei lavoratori – ai sensi dell'art. 4 dello Statuto dei Lavoratori – la quale prevede la possibilità di installare impianti e apparecchiature di controllo richiesti da esigenze organizzative o per fini di sicurezza soltanto previo accordo con le rappresentanze sindacali aziendali o previa autorizzazione della Direzione Provinciale del Lavoro. L'implementazione di tali misure dovrà, inoltre, avvenire nel rispetto dei doveri informativi prescritti dalle linee guida del Garante sull'utilizzo della posta elettronica e di Internet emanate il 1° marzo 2007.

Il Garante ha stabilito che la conservazione dei *file* di *log* delle operazioni di semplice consultazione (c.d. operazioni di *inquiry*) dei conti correnti, o di altri rapporti contrattuali riferiti ai clienti, dovrà essere garantita per un periodo non inferiore a 24 mesi dalla data di registrazione dell'operazione.

L'Autorità ha ritenuto inoltre necessario che le banche prevedano l'attivazione di specifici *alert* (avvisi) volti a rilevare comportamenti anomali o a rischio relativi alle operazioni di *inquiry* (semplice consultazione) eseguite dagli incaricati del trattamento (quali, ad esempio, intrusioni o accessi anomali e abusivi ai sistemi informativi).

La gestione dei dati bancari dovrà essere oggetto di un'attività di controllo interno da parte delle banche-titolari del trattamento con cadenza almeno annuale, in modo che sia verificata costantemente la conformità con le misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalla legge. I controlli dovranno comprendere anche verifiche periodiche sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati e sull'integrità dei dati e delle procedure informatiche adottate per il loro trattamento.

L'attività di controllo dovrà essere adeguatamente documentata, affinché sia sempre possibile risalire ai sistemi verificati, alle operazioni tecniche su di essi effettuate, alle risultanze delle analisi condotte sugli accessi e alle eventuali criticità riscontrate. L'esito delle attività di controllo dovrà essere poi richiamato nell'ambito del Documento Programmatico sulla Sicurezza e messo a disposizione del Garante, qualora ne faccia specifica richiesta.

Per concludere, l'Autorità ha indicato ulteriori misure opportune – e dunque suggerite, ma non imposte – al fine di contenere le conseguenze pregiudizievoli che potrebbero derivare da eventuali accessi non autorizzati ai dati personali dei clienti da parte dei dipendenti.

In tali casi, infatti, è previsto che le banche comunichino senza ritardo all'interessato le operazioni di trattamento illecito sui dati personali riferiti allo stesso, al fine di consentirgli di agire tempestivamente; comunicazione da indirizzare anche al Garante nei casi in cui risulti accertata una violazione di particolare rilevanza (in considerazione, ad esempio, della qualità o della quantità dei dati coinvolti, del numero di clienti interessati, etc.).

Per quanto 30 mesi siano un lasso temporale più che congruo per l'adozione delle misure prescritte, l'estrema rilevanza delle novità introdotte rende consigliabile sin da subito da parte delle banche un'attenta considerazione delle prescrizioni del Garante rispetto a qualsiasi futuro intervento sui sistemi informativi e sui processi organizzativi interni.