Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie - 12 maggio 2011 [1813953]

[doc. web n. 1813953]

[comunicato stampa]

[provvedimento di proroga: 18 luglio 2013]

Proroga del termine per l´adempimento delle prescrizioni di cui al Provvedimento n. 192 del 12 maggio 2011 in materia di circolazione delle informazioni bancarie - 22 maggio 2014

VEDI PROVVEDIMENTO DEL 30 LUGLIO 2019 SULLA NOTIFICA DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH)

Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie - 12 maggio 2011
(Pubblicato sulla Gazzetta Ufficiale n. 127 del 3 giugno 2011)

Registro dei provvedimenti
n. 192 del 12 maggio 2011

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Daniele De Paoli, segretario generale;

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

ESAMINATE le istanze (segnalazioni, reclami e quesiti) pervenute in tema di trattamento di dati personali della clientela effettuato dalle banche in ordine ai temi della "circolazione" delle informazioni riferite ai clienti all´interno dei gruppi bancari e della "tracciabilità" delle operazioni bancarie effettuate da incaricati del trattamento di tali dati (comprese quelle che non comportano movimentazione di denaro – c.d. inquiry);

VISTI i provvedimenti già adottati in tale ambito dall´Autorità;

RITENUTO di dover definire, in tale contesto, un quadro unitario di misure necessarie e opportune in grado di fornire ulteriori orientamenti utili per gli operatori del settore e i clienti, individuando, a tal fine, i comportamenti più appropriati da adottare;

RITENUTO che tali misure debbano essere oggetto di prescrizioni rese dal Garante ai sensi dell´art. 154, comma 1, lett. c) del Codice;

VISTE le osservazioni formulate dal segretario generale ai sensi dell´art. 15 del regolamento del

Garante n. 1/2000;

RELATORE il prof. Francesco Pizzetti;

PREMESSO

1. Profili generali.

1.1. Scopo del provvedimento.

Il presente provvedimento mira a fornire prescrizioni in relazione al trattamento di dati personali della clientela effettuato dai soggetti definiti al punto 1.2. al fine di garantire il rispetto dei princìpi in materia di protezione dei dai personali ai sensi del d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) in ordine ai temi della "circolazione" delle informazioni riferite ai clienti in ambito bancario e della "tracciabilità" delle operazioni bancarie effettuate dai dipendenti di istituti di credito (sia quelle che comportano movimentazione di denaro, sia quelle di sola consultazione, *c.d. inquiry*).

1.2. Ambito soggettivo di applicazione.

Il presente provvedimento si applica ai seguenti soggetti ove stabiliti sul territorio nazionale (art. 5 del Codice): alle banche, incluse quelle facenti parte di gruppi (disciplinati, in generale, dall´art. 2359 c.c. e, in particolare, dagli artt. 60 e ss. del d.lg. n. 385/1993); alle società, anche diverse dalle banche purché siano parte di tali gruppi (di seguito anch´esse denominate "banche"), nell´ambito dei trattamenti dalle stesse effettuati sui dati personali della clientela; a Poste Italiane S.p.A. (relativamente all´attività che gli operatori postali possono svolgere nell´ambito dei servizi bancari e finanziari ai sensi del d.P.R. 14 marzo 2001, n. 144 v. Regolamento recante norme sui servizi di bancoposta, adottato in attuazione della delega contenuta nell´art. 40 della l. 23 dicembre 1998, n. 448; v. anche Istruzioni di Vigilanza per le banche – Circ. Banca d´Italia n. 229 del 21 aprile 1999 - 10° Aggiornamento del 9 aprile 2004).

Il presente provvedimento si riferisce ai trattamenti effettuati dai soggetti sopra indicati mediante i propri dipendenti.

Restano salve le norme del Codice in materia di trasferimento dei dati all´estero da parte dei titolari del trattamento. In relazione a tale aspetto l´Autorità si riserva, qualora se ne dovesse ravvisare la necessità, di intervenire con un successivo provvedimento.

Il presente provvedimento, inoltre, non riguarda le modalità con le quali i clienti accedono on line ai servizi bancari (c.d. home banking).

1.3. Attività svolta.

Nel redigere il provvedimento si è tenuto conto delle istanze (segnalazioni, reclami e richieste di pareri) pervenute nel tempo in materia; degli accertamenti ispettivi effettuati, negli anni 2008, 2009 e 2010, presso le maggiori banche e/o gruppi bancari nazionali nonché presso Poste Italiane S.p.A.; degli specifici provvedimenti collegiali adottati dal Garante all´esito di alcuni di tali accertamenti; delle risultanze di un´ulteriore attività di indagine e rilevazione, svolta con la collaborazione dell´Associazione Bancaria Italiana (di seguito, ABI) e ultimata nel mese di ottobre 2010.

Con istanze rivolte all´Autorità, numerosi interessati hanno dichiarato di essere venuti a conoscenza che dati personali a loro riferiti (in specie, informazioni bancarie), conservati nei data base di alcune banche con le quali avevano instaurato rapporti contrattuali, erano stati oggetto di indebito accesso, verosimilmente da parte di alcuni dipendenti, i quali, successivamente, li avrebbero comunicati a terzi che li avrebbero utilizzati per scopi personali e, segnatamente, in vista di una loro produzione in giudizio (di norma, in separazioni giudiziali e procedure esecutive, in particolare, in pignoramenti presso terzi).

Considerata la rilevanza del tema, l´Autorità ha disposto accertamenti ispettivi presso alcuni istituti bancari volti a verificare, anzitutto, se effettivamente vi fossero stati accessi da parte di dipendenti alle informazioni bancarie dei clienti e i presupposti degli stessi.

All´esito dell´attività ispettiva svolta, sono emersi non solo elementi che hanno consentito di definire alcune segnalazioni con singole decisioni del Garante (*Provv.ti* 28 maggio 2009, doc. *web* n. 1624734; 18 giugno 2009, doc. *web* n. 1635720; 23 luglio 2009, doc. *web* n. 1640294; 18 marzo 2010, doc. *web* n. 1715015), ma anche profili problematici di carattere generale.

Inoltre, in ragione dell´accertata diversità di soluzioni organizzative adottate dalle banche e dell´elevato numero di soggetti coinvolti nell´indagine intrapresa, l´Autorità ha ritenuto necessario coinvolgere l´ABI in nuovi approfondimenti volti a chiarire ulteriormente le problematiche in esame.

Tali approfondimenti si sono concretizzati nella predisposizione, da parte dell´Autorità, di un questionario tipo, teso a rilevare le scelte organizzative effettuate dalle singole banche in relazione ai profili in questione, cui ha fatto riscontro un successivo documento elaborato dall´ABI in forma aggregata e anonima, da cui risulta che alla rilevazione hanno partecipato *"340 tra banche e gruppi bancari, che fanno complessivamente riferimento a 441 banche operanti sul territorio italiano"*.

2. La circolazione delle informazioni tra le banche appartenenti al gruppo.
2.1. Aspetti organizzativi emersi a seguito dell´attività istruttoria condotta.
La circolazione delle informazioni riferite alla clientela nell´ambito di un gruppo bancario può avvenire a diversi livelli astrattamente riconducibili a tre distinte tipologie:

1. la comunicazione di dati personali tra banche appartenenti al medesimo gruppo;

2. la circolazione di tali dati tra agenzie o filiali della stessa banca;

3. la circolazione di dati nell´ambito di una stessa agenzia o filiale.

Nella prima tipologia, relativa alla circolazione di dati personali della clientela tra banche appartenenti ad uno stesso gruppo, l´attività ispettiva svolta ha consentito di accertare che presso le singole realtà bancarie sono state effettuate scelte diversificate. In proposito sono state rilevate due fattispecie di seguito riportate:

• in un caso, tra le agenzie di diverse banche appartenenti al gruppo era prevista una circolarità limitata alle sole operazioni di versamento e prelevamento, senza avere mai la possibilità di conoscere il saldo contabile o la lista movimenti del conto acceso presso altro istituto del gruppo;

• in un altro caso, è emerso un regime di piena circolarità delle informazioni all´interno del gruppo bancario: la posizione del cliente e i suoi dati bancari erano accessibili dagli operatori di sportello designati incaricati del trattamento, in ragione delle funzioni svolte e dei profili di autorizzazione ad esse correlati, senza limitazioni.

Anche nella seconda tipologia, relativa alla circolazione delle informazioni tra agenzie o filiali della medesima banca, l´attività ispettiva ha fatto emergere notevoli differenze:

• in un caso, i dati dei clienti di una determinata agenzia sono risultati integralmente visibili per gli incaricati della stessa agenzia in possesso di adeguati profili di autorizzazione, i quali potevano non solo operare sui conti accesi presso la medesima, ma anche venire a conoscenza dell´esistenza di altri rapporti con lo stesso cliente presso altre agenzie della stessa banca, senza però poterne visualizzare l´effettiva consistenza patrimoniale. Nell´ambito delle agenzie appartenenti alla stessa banca, gli incaricati abilitati potevano effettuare, su richiesta di clienti titolari di rapporti incardinati presso altra agenzia, talune operazioni bancarie (versamento,

prelievo, bonifico, operazioni su titoli, ecc.) con possibilità di ottenere il saldo o la lista dei movimenti solo dopo la corretta effettuazione di una operazione di natura dispositiva;

• in un altro caso, gli incaricati non potevano effettuare operazioni di sportello, ad eccezione dei versamenti in contanti, in filiali diverse da quella presso la quale era gestito il conto corrente di uno specifico interessato. In tale ipotesi, la banca non operava in regime di circolarità, tranne che per le operazioni di visualizzazione dei dati bancari, che tutti gli addetti presso una specifica filiale potevano compiere in relazione ai dati bancari anche di clienti di altre filiali;

• in un ultimo caso, infine, si prevedeva che i dipendenti operanti all´interno di una filiale potessero accedere ai dati in esame limitatamente ai rapporti accesi presso la filiale medesima.

Nella terza tipologia, è stato rilevato che, generalmente, all´interno di una agenzia o filiale di una medesima banca la circolazione dei dati dei clienti avviene solo tra incaricati del trattamento in possesso di specifici profili di autenticazione e autorizzazione.

2.2. Profili di protezione dei dati personali.
Le risultanze istruttorie hanno evidenziato che le banche agiscono quali autonomi titolari del trattamento.

Da ciò consegue che il flusso di dati personali riferiti ai clienti nell´ambito di gruppi si configura come comunicazione a terzi.

Nell´informativa resa alla clientela, pertanto, ai sensi dell´art. 13 del Codice, ogni banca-titolare del trattamento deve indicare che i dati personali della clientela possono essere oggetto di comunicazione ad altri titolari del trattamento nell´ambito del medesimo gruppo bancario.

In relazione al profilo del consenso, si rileva che la comunicazione di dati, in tale ambito, è possibile solo ove sia stato acquisito il consenso informato dell´interessato (art. 23 del Codice) o si sia in presenza di uno dei presupposti di esonero del consenso previsti dall´art. 24 del Codice.

Al contrario, il flusso di dati tra diverse agenzie o filiali di una stessa banca costituisce circolazione di informazioni all´interno di un unico titolare del trattamento e, non configurando un´operazione di comunicazione di dati a terzi, non richiede il consenso degli interessati.

L´informativa, tuttavia, potrà contenere anche l´indicazione che i dati della clientela potranno circolare tra le agenzie o filiali di ciascuna banca.

3. La circolazione delle informazioni tra le banche del gruppo e i soggetti che gestiscono i sistemi informativi contenenti dati bancari della clientela.
***3.1. Aspetti organizzativi emersi a seguito dell´attività istruttoria condotta*.**
Sotto il profilo organizzativo, all´esito dell´attività ispettiva è emerso che i sistemi informativi contenenti i dati relativi alla clientela delle banche, mediante i quali vengono registrati gli accessi dei dipendenti a tali dati, sono gestiti da società (interne o esterne alla compagine di gruppo) con le quali ciascuna banca stipula appositi contratti di servizio. In proposito, l´ABI ha individuato due tipologie organizzative:

1. gruppi bancari caratterizzati da una gestione prevalentemente interna del sistema informativo […] affidata a una società di servizio appartenente al gruppo bancario, che si configura come soggetto terzo Responsabile o, in alcuni casi, Titolare del trattamento dei dati personali […];

2. gruppi bancari/banche caratterizzati da una gestione prevalentemente esterna del sistema informativo […] caratterizzati da un elevato livello di outsourcing, in relazione alla gestione del sistema informativo. In questo caso, la banca titolare del trattamento, esternalizzando la gestione dei dati, designa il soggetto terzo "responsabile del trattamento".

Nell´ambito della prima tipologia organizzativa, l´ABI ha evidenziato che la c.d. società "strumentale", nella maggior parte dei casi, assume la veste di titolare autonomo del trattamento dei dati della clientela; sono anche presenti, tuttavia, casi residuali di designazione della stessa come responsabile del trattamento.

Nell´ambito di tale tipologia si possono evidenziare due ulteriori sottocategorie:

a) le realtà bancarie di grandi dimensioni, ove la gestione dei sistemi informativi è affidata a una società "strumentale" interna al gruppo che può assumere diverse forme -tra cui quella del consorzio- e che può avvalersi di soggetti terzi per la gestione di talune attività soprattutto di carattere infrastrutturale;

b) le realtà bancarie di medie dimensioni, ove si configurano sistemi informativi in alcuni casi analoghi a quelli descritti alla precedente lettera a), in altri casi centralizzati presso la capogruppo.

Nell´ambito della seconda tipologia organizzativa descritta dall´ABI, la gestione del sistema informativo mediante il quale vengono effettuate operazioni di trattamento dei dati personali della clientela della banca è affidata, in prevalenza, a un unico soggetto terzo (solo in casi limitati sono previsti anche più soggetti, in genere in numero non superiore a due) che "partecipa alle attività di trattamento e gestione delle informazioni sulla base di una serie di servizi elencati e concordati nell´ambito di accordi contrattuali, definiti in funzione delle specifiche esigenze della singola banca".

3.2. Profili di protezione dei dati personali.
Le differenti soluzioni adottate dalle banche e dai gruppi bancari in coerenza con le proprie specifiche caratteristiche, anche dimensionali e operative rendono opportuno formulare alcune prescrizioni in merito alle modalità attraverso le quali ciascuna banca o gruppo bancario può garantire la trasmissione alla società che gestisce i sistemi informativi dei dati personali relativi ai clienti. Alla luce dell´esame complessivo delle risultanze istruttorie, si deve ritenere che la qualificazione delle società che gestiscono i sistemi informativi (di seguito denominati semplicemente "outsourcer") quali autonomi "titolari del trattamento" (con tutte le conseguenze che ciò comporta anche in termini di eventuale responsabilità civile nei confronti degli interessati) spesso può risultare non conforme alle previsioni del Codice (e, segnatamente, agli artt. 4, comma 1, lett. f) e g), 28 e 29).

Infatti, benché l´esternalizzazione dei sistemi informativi costituisca una libera scelta organizzativa di esclusiva pertinenza delle banche, affinché i connessi trattamenti di dati personali dei clienti risultino conformi alla disciplina sulla protezione dei dati personali, è indispensabile che ciascuna banca valuti attentamente se le società di gestione di detti sistemi (a prescindere dal fatto che si tratti di soggetti interni o esterni alla compagine di gruppo o alla singola banca), alla luce delle specifiche attività che sono chiamate a svolgere in base ai contratti di servizio, possano essere effettivamente considerate quali autonomi titolari o non vadano invece designate quali "responsabili" del trattamento ai sensi dell´art. 29 del Codice (in questo senso v. anche il parere del Gruppo Art. 29 sulla protezione dei dati, n. 1/2010 -WP 169- del 16 febbraio 2010).

Infatti, la posizione di "titolare" del trattamento, pur astrattamente riconoscibile anche in capo all´outsourcer, risulta, tuttavia, ascrivibile solo alla banca nei casi in cui la stessa abbia il potere di:

1. assumere decisioni relative alle finalità del trattamento;

2. impartire istruzioni e direttive vincolanti nei confronti delle società di gestione dei sistemi informativi, sostanzialmente corrispondenti alle istruzioni che il titolare del trattamento deve impartire al responsabile;

3. svolgere funzioni di controllo rispetto all´operato delle medesime e degli incaricati delle stesse.

Alla luce di tali considerazioni, quando il trattamento di dati personali dei clienti da parte dell´outsourcer è svolto restando riservati alle banche i poteri -sopra indicati- riconosciuti dal Codice solo al titolare (artt. 4, comma 1, lett. f) e 28) e dunque, in concreto, detti poteri, non risultino effettivamente posti in capo all´outsourcer, le banche devono essere considerate gli unici titolari del trattamento, con conseguente necessità di designare le società operanti in outsourcing quali responsabili (artt. 4, comma 1, lett. g) e 29, commi 4 e 5 del Codice).

4. Il "tracciamento" delle operazioni di accesso ai dati e gli strumenti di audit.

4.1. Aspetti organizzativi emersi a seguito dell´attività istruttoria.

In relazione al profilo degli accessi informatici da parte dei dipendenti delle banche ai dati relativi alla clientela e al correlato tracciamento delle operazioni poste in essere dagli stessi, si ritiene di dover formulare alcune prescrizioni.

Le diverse soluzioni adottate da ciascuna banca o gruppo bancario, oggetto di accertamento in loco in ordine alle caratteristiche tecnologiche dei sistemi informativi con cui vengono tracciate le operazioni bancarie (sia dispositive, sia di semplice *inquiry*), sono espressione della discrezionalità riconosciuta a ciascuna banca o gruppo bancario nel dare attuazione a quanto previsto nelle "Disposizioni di vigilanza per le banche in materia di conformità alle norme (*compliance*)", adottate dalla Banca d´Italia il 10 luglio 2007. In linea con gli orientamenti emersi in sede internazionale, le Istruzioni di vigilanza definiscono ruolo e responsabilità degli organi di vertice delle banche e prevedono la costituzione della funzione di compliance, quale elemento integrante del sistema dei controlli interni. Tale funzione, istituita per la prima volta proprio con le citate disposizioni, è preposta al presidio e alla gestione del rischio di incorrere in sanzioni amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme imperative o di autoregolamentazione (rischio di compliance). Le disposizioni stabiliscono i principali compiti e i requisiti qualitativi minimi della funzione di compliance, le attribuzioni del suo responsabile, le interrelazioni con le altre funzioni aziendali (in particolare con la funzione di controllo interno, c.d*. internal auditing*).

Tale funzione, preposta al controllo interno nelle banche, è disciplinata dalla legge e da un quadro di norme regolamentari emanate dalla Banca d´Italia mediante apposite istruzioni, in particolare, le Istruzioni di vigilanza in materia di "Organizzazione e controlli interni". Queste ultime richiedono alle banche di dotarsi di sistemi di monitoraggio dei rischi aziendali e di verifica dell´affidabilità e della sicurezza, anche dei sistemi informativi, istituendo indicatori di anomalie (c.d. *alert*) per orientare successivi interventi di audit.

In assenza di disposizioni normative recanti obblighi in materia di tracciabilità delle operazioni bancarie con riguardo sia all´an sia al quantum della conservazione dei file di log, si rileva che, nell´ambito della discrezionalità riconosciuta alle banche nell´organizzare la funzione di compliance, tutte le banche sottoposte ad attività ispettiva hanno ritenuto di implementare sistemi di controllo delle operazioni dispositive con finalità di tutela del patrimonio dei clienti e dell´attività bancaria, ma solo alcune di esse sono risultate in possesso di sistemi di tracciamento riguardanti anche operazioni di semplice consultazione (*inquiry*) dei conti correnti o di altri rapporti contrattuali riferiti ai clienti. Anche in quest´ultimo caso, a causa di tempi di conservazione dei file di log troppo ristretti, tuttavia non è stato sempre possibile risalire ai dettagli di un´operazione di accesso ai dati posta in essere da un incaricato.

Al riguardo, nel prendere atto dell´assenza di disposizioni normative in tale ambito, si ritiene opportuno prescrivere alcune misure in ordine a:

• "tracciamento" degli accessi ai dati bancari dei clienti;

• tempi di conservazione dei relativi file di log;

• implementazione di alert volti a rilevare intrusioni o accessi anomali ai dati bancari, tali da configurare eventuali trattamenti illeciti;

4.2. Il "tracciamento" degli accessi ai sistemi e i tempi di conservazione dei relativi file di log.

4.2.1. Tracciamento delle operazioni.
Al fine di assicurare il controllo delle attività svolte sui dati dei clienti e dei potenziali clienti da ciascun incaricato del trattamento (quali che siano la sua qualifica, le sue competenze e gli ambiti di operatività e le finalità del trattamento che è tenuto a svolgere) devono essere adottate idonee soluzioni informatiche. Oltre alle misure minime di sicurezza, già prescritte dall´art. 34 del Codice nel caso di trattamento di dati personali effettuato con strumenti elettronici (con particolare riguardo alla necessità di "protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti […]" di cui alla lett. e) del citato art. 34), è necessario implementare misure idonee (art. 31 del Codice) che permettano un efficace e dettagliato controllo anche in ordine ai trattamenti condotti sui singoli elementi di informazione presenti nei diversi database utilizzati.

Tali soluzioni comprendono la registrazione dettagliata, in un apposito log, delle informazioni riferite alle operazioni bancarie effettuate sui dati bancari, quando consistono o derivano dall´uso interattivo dei sistemi operato dagli incaricati, sempre che non si tratti di consultazioni di dati in forma aggregata non riconducibili al singolo cliente.

In particolare, i file di *log* devono tracciare per ogni operazione di accesso ai dati bancari effettuata da un incaricato, almeno le seguenti informazioni:

• il codice identificativo del soggetto incaricato che ha posto in essere l´operazione di accesso;

• la data e l´ora di esecuzione;

• il codice della postazione di lavoro utilizzata;

• il codice del cliente interessato dall´operazione di accesso ai dati bancari da parte dell´incaricato;

• la tipologia di rapporto contrattuale del cliente a cui si riferisce l´operazione effettuata (es. numero del conto corrente, fido/mutuo, deposito titoli).

Le misure di cui al presente paragrafo sono adottate nel rispetto della vigente disciplina in materia di controllo a distanza dei lavoratori (art. 4, l. 20 maggio 1970, n. 300), tenendo altresì conto dei princìpi affermati dal Garante in tema di informativa agli interessati nelle linee guida sull´utilizzo della posta elettronica e di internet (*Provv*. 1° marzo 2007, doc. *web* n. 1387522).

4.2.2. Conservazione dei log di tracciamento delle operazioni.
Il periodo di conservazione dei file di log che tracciano gli accessi varia in base alla tipologia di *log* memorizzato; inoltre, fatta eccezione per quelli che tracciano gli accessi degli amministratori di sistema (per i quali è previsto un periodo minimo di conservazione di 6 mesi; v. punto 4.5 del Provv. 27 novembre 2008, doc. *web* n. 1577499), per gli altri *log* non sono normativamente prescritti tempi di conservazione. Anche le risultanze istruttorie hanno confermato che i log sono conservati per un periodo variabile (in tal senso è anche la documentazione prodotta dall´ABI, che rileva come i log di accesso ai sistemi informativi siano conservati mediamente per 12 mesi, mentre i log file delle transazioni bancarie sono conservati per un periodo non inferiore a 10 anni).

Tuttavia, alla luce dell´esperienza maturata in sede ispettiva, si ritiene congruo stabilire che i *log* di tracciamento delle operazioni di inquiry siano conservati per un periodo non inferiore a 24 mesi dalla data di registrazione dell´operazione. Ciò in quanto un periodo di tempo inferiore non consentirebbe agli interessati di venire a conoscenza dell´avvenuto accesso ai propri dati personali e delle motivazioni che lo hanno determinato.

4.3. L´implementazione di alert volti a rilevare intrusioni o accessi anomali e abusivi ai sistemi informativi.

4.3.1. Implementazione di alert.

Deve essere prefigurata da parte delle banche l´attivazione di specifici alert che individuino comportamenti anomali o a rischio relativi alle operazioni di inquiry eseguite dagli incaricati del trattamento.

Anche a tal fine, negli strumenti di business intelligence utilizzati dalle banche per monitorare gli accessi alle banche dati contenenti dati bancari devono confluire i log relativi a tutti gli applicativi utilizzati per gli accessi da parte degli incaricati del trattamento.

4.3.2. Audit interno di controllo–Rapporti periodici.
La gestione dei dati bancari deve essere oggetto, con cadenza almeno annuale, di un´attività di controllo interno da parte dei titolari del trattamento, in modo che sia verificata costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

L´attività di controllo deve essere demandata a un´unità organizzativa o, comunque, a personale diverso rispetto a quello cui è affidato il trattamento dei dati bancari dei clienti.

I controlli devono comprendere anche verifiche a posteriori, a campione, o a seguito di allarme derivante da sistemi di *alerting* e di *anomaly detection*, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull´integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte, altresì, verifiche periodiche sulla corretta conservazione dei file di log per il periodo previsto al punto 4.2.2.

L´attività di controllo deve essere adeguatamente documentata in modo tale che 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 dell´attività di controllo deve essere:

• comunicato alle persone e agli organi legittimati ad adottare decisioni e a esprimere, a vari livelli in base al proprio ordinamento interno, la volontà della banca;

• richiamato nell´ambito del documento programmatico sulla sicurezza nel quale devono essere indicati gli interventi eventualmente necessari per adeguare le misure di sicurezza;

• messo a disposizione del Garante, in caso di specifica richiesta.

5. Informazioni in caso di accessi non autorizzati.
5.1. Informazioni all´interessato.
Le banche comunicano senza ritardo all´interessato le operazioni di trattamento illecito effettuate -sui dati personali allo stesso riferiti- dagli incaricati. Tale tempestiva informazione, infatti, in termini generali, può consentire all´interessato l´adozione di appropriate misure e, ove possibile, una minimizzazione dei rischi connessi alla violazione della disciplina di protezione dei dati personali.

Tale comunicazione costituisce misura opportuna ai sensi dell´art. 154, comma 1, lett. c) del Codice.

5.2. Comunicazioni al Garante.
Le banche comunicano tempestivamente al Garante fornendo gli opportuni dettagli i casi in cui

risultino accertate violazioni, accidentali o illecite, nella protezione dei dati personali, purché di particolare rilevanza per la qualità o la quantità di dati coinvolti e/o il numero di clienti interessati, dalle quali derivino la distruzione, la perdita, la modifica, la rivelazione non autorizzata dei dati della clientela.

Tale comunicazione costituisce misura opportuna ai sensi dell´art. 154, comma 1, lett. c) del Codice.

TUTTO CIÒ PREMESSO, IL GARANTE

ai sensi dell´art. 154, comma 1, lett. c) del Codice, prescrive le misure di seguito indicate alle banche, incluse quelle facenti parte di gruppi; alle società diverse dalle banche, purché siano parte di tali gruppi; a Poste Italiane S.p.A. nell´esercizio dell´attività di cui al punto 1.2. del presente provvedimento:

1) Misure necessarie:

a) Designazione dell´*outsourcer* quale responsabile del trattamento (punto 3.2).
Quando il trattamento di dati personali dei clienti da parte di outsourcer è svolto restando riservati alle banche i poteri riconosciuti dal Codice solo al titolare (artt. 4, comma 1, lett. f) e 28), e dunque, in concreto, detti poteri, non risultino posti effettivamente in capo all´*outsourcer*, le stesse banche, quali unici titolari del trattamento, devono designare le società operanti in *outsourcing* responsabili ai sensi degli artt. 4, comma 1, lett. g) e 29, commi 4 e 5 del Codice.

b) Tracciamento delle operazioni (punto 4.2.1).
Devono essere adottate idonee soluzioni informatiche per il controllo dei trattamenti condotti sui singoli elementi di informazione presenti sui diversi database. Tali soluzioni comprendono la registrazione dettagliata, in un apposito log, delle informazioni riferite alle operazioni bancarie effettuate sui dati bancari, quando consistono o derivano dall´uso interattivo dei sistemi operato dagli incaricati, sempre che non si tratti di consultazioni di dati in forma aggregata non riconducibili al singolo cliente.

In particolare, i file di log devono tracciare per ogni operazione di accesso ai dati bancari effettuata da un incaricato, almeno le seguenti informazioni:

• il codice identificativo del soggetto incaricato che ha posto in essere l´operazione di accesso;

• la data e l´ora di esecuzione;

• il codice della postazione di lavoro utilizzata;

• il codice del cliente interessato dall´operazione di accesso ai dati bancari da parte dell´incaricato;

• la tipologia di rapporto contrattuale del cliente a cui si riferisce l´operazione effettuata (es. numero del conto corrente, fido/mutuo, deposito titoli).

c) Conservazione dei *log* di tracciamento delle operazioni (punto 4.2.2).

Il periodo di conservazione dei file di log delle operazioni di inquiry non deve essere inferiore a 24 mesi dalla data di registrazione dell´operazione.

d) Implementazione di *alert* (punto 4.3.1).

i. Deve essere prefigurata da parte delle banche l´attivazione di specifici *alert* che individuino comportamenti anomali o a rischio relativi alle operazioni di inquiry.

ii. Negli strumenti di *business intelligence* devono confluire i *log* relativi a tutti gli applicativi utilizzati per gli accessi.

e) *Audit* interno di controllo–Rapporti periodici (punto 4.3.2).

i. La gestione dei dati bancari deve essere oggetto, con cadenza almeno annuale, di un´attività di controllo interno da parte dei titolari del trattamento.

ii. L´attività di controllo deve essere demandata a un´unità organizzativa o, comunque, a personale diverso rispetto a quello cui è affidato il trattamento dei dati bancari dei clienti.

iii. I controlli devono comprendere anche verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di alerting e di anomaly detection, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull´integrità dei dati e delle procedure informatiche adoperate per il loro trattamento. Sono svolte, altresì, verifiche periodiche sulla corretta conservazione dei file di log per il periodo previsto al punto 4.2.2.

iv. L´attività di controllo deve essere adeguatamente documentata e il relativo esito deve essere comunicato ai soggetti indicati al punto 4.3.2.

2) Misure opportune:

f) Informativa all´interessato (punto 2.2).

L´informativa resa all´interessato ai sensi dell´art. 13 del Codice, potrà contenere anche l´indicazione che i dati della clientela potranno circolare tra le agenzie o filiali di ciascuna banca.

g) Informazioni all´interessato (punto 5.1).

Le banche comunicano, senza ritardo, all´interessato le operazioni di trattamento illecito effettuate -sui dati personali allo stesso riferiti- dagli incaricati.

h) Comunicazioni al Garante (punto 5.2).

Le banche comunicano tempestivamente al Garante i casi in cui risulti accertata una violazione, accidentale o illecita, nella protezione dei dati personali, di particolare rilevanza.

3) dispone, che le misure di cui al punto 1) del presente dispositivo, siano adottate entro 30 mesi dalla pubblicazione del presente provvedimento sulla *Gazzetta Ufficiale*;

4) dispone, ai sensi dell´art. 143, comma 2, del Codice, di trasmettere al Ministero della giustizia-Ufficio pubblicazione leggi e decreti copia del presente provvedimento, per la relativa pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 12 maggio 2011

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
De Paoli