PROVVEDIMENTO 27 ottobre 2005
Trattamento di alcuni dati personali (immagini e impronte digitali) da parte di banche. (G.U. n. 68 del 22.03.2006)

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. Giovanni Buttarelli, segretario generale;
Vista la normativa internazionale e comunitaria in materia di protezione dei dati personali (direttiva n. 95/46/CE);
Visto il Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196), con particolare riguardo all'art. 17;
Visti i provvedimenti del Garante del 29 aprile 2004, in materia di videosorveglianza, e del 28 settembre 2001, relativo alle rilevazioni biometriche presso gli istituti di credito;
Esaminate le richieste di verifica preliminare presentate da vari istituti di credito ai sensi dell'art. 17 del Codice, relative al trattamento di dati personali biometrici in relazione ad esigenze di sicurezza presso sportelli bancari; vista la bozza di linee-guida che l'Associazione bancaria italiana intende inoltrare alle banche e che ha sottoposto all'attenzione di questa Autorita';
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. Introduzione.
Alcuni istituti di credito hanno inoltrato a questa Autorita' una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, relativa a trattamenti di dati personali consistenti nell'associazione di dati biometrici di clienti (risultanti, in particolare, dall'acquisizione di impronte digitali tramite scanner collegati o integrati in un sistema informatico) con altri dati personali, relativi anch'essi alla clientela, raccolti avvalendosi di sistemi di ripresa.
Le richieste sono state presentate, anche in relazione a quanto prescritto dal Garante con il provvedimento in materia di videosorveglianza del 29 aprile 2004 (punto 3.2.1), per consentire la raccolta di elementi di prova suscettibili di utilizzazione in caso di comportamenti delittuosi.
L'Associazione bancaria italiana, nel fornire alcuni dati statistici relativi a fenomeni criminosi posti in essere nei confronti di dipendenze bancarie (in particolare, a rapine), ha rappresentato a sua volta che l'esigenza di dotare di impianti di rilevazione biometrica talune filiali maggiormente esposte alla commissione di reati e' condivisa da una pluralita' di istituti.
All'esito della complessa istruttoria preliminare, il Garante ritiene necessario adottare un nuovo provvedimento di carattere generale che, sulla base dei principi generali gia' enunciati nel provvedimento del 28 settembre 2001 (in Bollettino n. 22/2001, p. 82), tenga conto delle novita' sopravvenute con il Codice entrato in vigore il 1° gennaio 2004 (con particolare riguardo alle disposizioni contenute negli articoli 17, 24, comma 1, lettera g) e 154, comma 1, lettera c)). In relazione ai trattamenti di dati personali (diversi da quelli sensibili e giudiziari) che presentano rischi specifici per

i diritti e le liberta' fondamentali, nonche' per la dignita' dell'interessato, il Garante ha infatti il compito di individuare misure ed accorgimenti rivolti «a determinate categorie di titolari o di trattamenti» nell'ambito di una verifica preliminare all'inizio del trattamento (art. 17 del Codice).
Nel caso in esame (come gia' rilevato nel menzionato punto 3.2.1. del provvedimento del 2004), i rischi specifici sono determinati dall'installazione di «sistemi di videosorveglianza che prevedono una raccolta delle immagini collegata e/o incrociata e/o confrontata con altri particolari dati personali», e dalla particolare natura di alcuni dati trattati, segnatamente di quelli derivanti dalla rilevazione delle impronte digitali.
Il presente provvedimento mira, pertanto, ad individuare le misure e gli accorgimenti a garanzia degli interessati che dovranno essere posti in essere da tutti gli istituti di credito operanti sul territorio nazionale che intendano avvalersi dei sistemi descritti, qualora ne ricorrano i presupposti di seguito indicati e rispettando i principi contenuti nel Codice.
2. Liceita', finalita', necessita' e proporzionalita'.
L'utilizzo generalizzato ed indiscriminato di sistemi che consentono l'identificazione degli interessati mediante la combinazione di diversi sistemi di rilevazione dati non e' consentito, in quanto contrasta con il principio di necessita' che impone di configurare i sistemi informativi e i programmi informatici escludendo il trattamento di dati personali non necessari - nel caso di specie, biometrici - in rapporto alle finalita' che si intende perseguire (art. 3 del Codice).
Un'attivita' di raccolta indifferenziata di dati particolarmente significativi (quali quelli relativi alle impronte digitali), imposta all'intera clientela degli istituti bancari, non e' lecita, tanto piu' se giustificata solo da una generica esigenza di sicurezza.
In mancanza di specifici elementi che comprovino una concreta situazione di elevato rischio, tale attivita' comporta infatti un sacrificio sproporzionato della sfera di liberta' e della dignita' delle persone interessate, esponendo, altresi', le stesse a pericolo di abusi in relazione a dati a se' riferibili particolarmente delicati quali sono le impronte digitali.
Il trattamento di tali dati personali e' consentito, con l'osservanza di adeguate garanzie, soltanto quando debba essere perseguita l'esclusiva finalita' di elevare il grado di sicurezza di beni e persone (segnatamente, del personale dipendente degli istituti di credito e della clientela). A tal fine e' necessaria la ricorrenza di specifici elementi riconducibili a circostanze obiettive che devono evidenziare una concreta situazione di elevato rischio e che l'istituto bancario deve valutare con particolare cautela (cfr. Provv. 11 dicembre 2000, in Boll. n. 14-15/2000, p. 30; Provv. 7 marzo 2001).
Tali particolari condizioni, risultanti anche da concordanti valutazioni da parte degli organi competenti in materia di tutela dell'ordine e della sicurezza pubblica, possono derivare, in particolare, dalla localizzazione dello sportello bancario (ad esempio, ove lo stesso sia situato in aree ad alta densita' criminale, o isolate o, comunque, poste nell'immediata prossimita' di «vie di fuga»). Puo' altresi' venire in considerazione la circostanza che lo sportello bancario, o altri sportelli siti nella medesima zona, abbiano subito rapine. Possono inoltre rilevare altre contingenti vicende che espongano a reale pericolo una o piu' filiali determinate (come ad esempio rilevato in passato, con riguardo alla maggiore «liquidita» presso gli sportelli bancari in corrispondenza

dell'introduzione della moneta unica europea: cfr. Provv. 28 settembre 2001).
La sussistenza di tali circostanze deve essere altresi' valutata periodicamente in rapporto a fattori suscettibili di incidere sulla soglia di esposizione a rischio (si pensi, ad esempio, all'istituzione di una postazione di pubblica sicurezza nelle immediate vicinanze, oppure al rafforzamento di servizi di sorveglianza privata all'interno della filiale). All'esito di tale valutazione periodica i trattamenti di dati non piu' giustificati devono essere cessati o sospesi.
3. Informativa.
Gli interessati devono essere informati adeguatamente della presenza dei sistemi di acquisizione delle impronte digitali e dell'associazione di queste ultime con immagini raccolte (art. 13 del Codice). Cio', prima che i dati siano rilevati e, comunque, prima dell'accesso a varchi a doppia porta o bussole.
L'informativa deve fornire gli elementi previsti dal Codice (art. 13) anche con formule sintetiche, ma chiare e senza ambiguita'. Deve essere ben evidenziata la liberta' di accedere in banca senza consentire il rilevamento dell'impronta digitale, sulla base di un procedimento alternativo basato anche su un'identificazione del cliente eventualmente necessaria.
Il Garante ha individuato un modello di informativa «minima» che i titolari del trattamento potranno utilizzare in corrispondenza dei varchi di accesso alle strutture della banca, che dovra' essere integrato con un'informativa piu' ampia esposta all'interno della dipendenza bancaria. Entrambi i modelli sono allegati in facsimile al presente provvedimento.
4. Misure ed accorgimenti.
L'utilizzazione dei sistemi di rilevazione delle impronte digitali associata a sistemi di videosorveglianza deve avvenire nel rispetto degli ulteriori accorgimenti e misure a garanzia degli interessati, di seguito elencati.
a) modalita' alternative di accesso alla banca.
La rilevazione delle impronte digitali non puo' comportare una contrazione della liberta' e della dignita' degli utenti degli sportelli bancari. L'accesso tramite i descritti sistemi di rilevazione deve avvenire predisponendo un meccanismo che, in presenza di una difforme volonta' del cliente, oppure dell'impossibilita' del medesimo di prestarsi alle operazioni di trattamento in ragione di proprie condizioni personali, gli permetta di accedere comunque all'istituto bancario attraverso un ingresso alternativo (o comunque senza dover essere obbligato a rilasciare dati personali), con l'eventuale adozione di cautele rimesse alla ragionevole valutazione dei responsabili della filiale (come, ad esempio, con la richiesta di esibizione di un documento). Come gia' rilevato nel richiamato provvedimento del 2001, sono da ritenersi precluse eventuali pratiche vessatorie o comunque elusive dell'obbligo di consentire l'ingresso senza rilevazione dell'impronta.
b) modalita' di raccolta.
I sistemi di videosorveglianza installati devono essere orientati esclusivamente verso l'area di accesso all'istituto di credito, senza riprendere altri immobili e, in particolare, i loro ingressi.
Quanto ai dati biometrici da raccogliere, e' sufficiente rilevare solo l'impronta dattiloscopica di una delle dita dell'interessato.
c) misure di sicurezza.
I sistemi per la raccolta delle immagini (fisse o in movimento) e delle impronte digitali devono prevedere l'immediata cifratura dei

dati, prima della loro registrazione in una banca dati comunque configurata, e devono garantire un livello elevato di sicurezza.
Deve essere assicurata l'associazione univoca tra le immagini e le impronte digitali, per evitare errori di identificazione.
Particolare attenzione deve essere dedicata alle tecniche crittografiche applicate alle immagini e alle impronte.
I dati devono essere trattati con sistemi di cifratura «robusti» con l'utilizzo, anche congiunto, di algoritmi crittografici simmetrici o asimmetrici.
In particolare, qualora si ricorra a tecniche di crittografia simmetrica per la cifratura dei dati e a crittografia asimmetrica o a chiave pubblica per la cifratura delle chiavi simmetriche relative a ciascun dato o a ciascuna porzione di dato, l'intero processo crittografico deve essere garantito dall'interposizione di un vigilatore dei dati (individuato nel titolare di una funzione di controllo interno in posizione di indipendenza, o da un soggetto parimenti indipendente da questi designato), depositario delle chiavi crittografiche idonee a decifrare le informazioni conservate dalla banca.
Deve essere infatti evitata la possibilita', anche solo tecnica, di decifrare le informazioni acquisite senza l'intervento del predetto vigilatore dei dati.
L'accesso alle informazioni «in chiaro», sia per esigenze di giustizia, sia in caso di esercizio dei diritti dell'interessato (art. 7 del Codice), deve avvenire solo tramite il medesimo vigilatore dei dati.
Resta fermo l'obbligo di adottare, in conformita' al Codice, misure di sicurezza anche minime corrispondenti ai parametri previsti (art. 31 ss. e Allegato B del Codice), in particolare per quanto riguarda l'accesso degli incaricati o amministratori di sistema che abbiano un ruolo nella conduzione o nella manutenzione dei sistemi utilizzati.
I sistemi di rilevazione devono infine offrire una garanzia rigorosa di affidabilita' e di integrita' dei dati, anche sulla base di eventuali certificazioni od omologazioni dei dispositivi. In questa cornice, gli istituti presso i quali vengono installati i sistemi oggetto del presente provvedimento devono farsi rilasciare dall'installatore, e conservare, l'attestato di cui alla regola n. 25 del disciplinare tecnico in materia di misure minime di sicurezza (Allegato «B» al Codice).
d) conservazione dei dati.
I dati cifrati relativi alle impronte e alle eventuali immagini devono essere conservati per un periodo non superiore ad una settimana e devono essere registrati cronologicamente in modo tale da consentire il loro pronto reperimento anche sulla base di un'opportuna organizzazione per giorni di rilevazione.
Devono essere predisposti meccanismi di integrale cancellazione automatica delle informazioni allo scadere del termine previsto. Deve essere altresi' evitato un prolungamento surrettizio dei tempi di conservazione attraverso la creazione di copie di sicurezza.
Resta fermo che la banca, in presenza di una richiesta di accesso da parte dell'interessato, oppure di eventi criminosi verificatisi o, ancora, di una richiesta da parte dell'autorita' giudiziaria, potra' assicurare la disponibilita' dei dati raccolti, evitandone l'automatica cancellazione alla scadenza del periodo di conservazione previsto.
Da ultimo, non puo' ritenersi consentito alcun sistema di interconnessione dei dati raccolti con altri dati in possesso dell'istituto bancario o di terzi, o di creazione di ulteriori database, come pure di sistemi di riconoscimento facciale.

e) conoscibilita' dei dati.
Possono decifrare ed accedere alle informazioni raccolte con i sistemi di rilevazione soltanto le autorita' giudiziarie e di polizia, con riferimento a specifiche attivita' investigative connesse all'accertamento o alla prevenzione di reati svolte in conformita' al codice di procedura penale. Cio', avvalendosi anche della cooperazione del predetto vigilatore dei dati, il quale puo', se necessario, venire lecitamente a conoscenza di dati qualora presti la propria opera anche in caso di esercizio del diritto d'accesso da parte dell'interessato ai dati personali a se' riferiti.
Il personale, anche esterno alla banca, selettivamente preposto all'utilizzo e alla manutenzione delle apparecchiature, non deve invece poter accedere in alcun modo «in chiaro» alle informazioni cifrate (immagini ed impronte).
5. Bilanciamento di interessi.
In presenza dei presupposti e delle condizioni sopra indicati, il trattamento dei dati personali potra' ritenersi lecito anche in assenza del consenso degli interessati, ai sensi dell'art. 24, comma 1, lettera g), del Codice.
Cio', attesa la particolare finalita' perseguita e considerando sia la temporaneita' e le modalita' del trattamento da effettuarsi nella rigorosa osservanza delle misure e degli accorgimenti prescritti con il presente provvedimento, sia le ulteriori finalita' perseguite dagli altri titolari del trattamento ai quali i dati possono essere comunicati (identificati nell'autorita' giudiziaria e nelle forze di polizia).
Il consenso dell'interessato deve ritenersi non necessario anche con riguardo alle operazioni di decrittazione dei dati trattati ad opera del vigilatore dei dati, le cui ulteriori operazioni di trattamento devono esaurirsi nella sola comunicazione dei dati «in chiaro» ai soggetti sopra individuati o all'interessato che abbia esercitato il diritto d'accesso riconosciutogli dall'art. 7 del Codice.
6. Adempimenti.
Resta in primo luogo fermo l'obbligo di notificare al Garante il trattamento dei dati secondo le modalita' previste (art. 37, comma 1, lettera a) del Codice).
Ciascun istituto di credito e' altresi' tenuto ad inviare a questa Autorita', entro il 31 gennaio 2006 e con un'unica comunicazione riguardante tutti i propri sportelli bancari, l'elenco di quelli per i quali i dispositivi in esame siano stati gia' attivati prima del presente provvedimento.
Ogni istituto di credito che intenda installare nuove apparecchiature, oppure modificare quelle esistenti, dovra' invece inoltrare, sempre al Garante, una specifica richiesta di verifica preliminare utilizzando i modelli riprodotti in allegato, verifica da svolgere una tantum ai sensi dell'art. 17 del Codice, prima dell'inizio del trattamento. A tal fine potra' essere effettuata un'unica comunicazione riguardante tutti gli sportelli della banca, indicando l'elenco di quelli per i quali intende attivare i dispositivi menzionati e le condizioni di concreto rischio poste a fondamento della loro installazione valutate in rapporto alle altre misure adottabili.
Da ultimo, in aggiunta alle predette prescrizioni, presso ogni sportello bancario dovra' essere comunque conservata e tenuta aggiornata, anche in previsione di verifiche disposte da questa Autorita', la seguente documentazione:
a) copia della richiesta di verifica preliminare inviata al Garante;

b) eventuale documentazione dalla quale si possa desumere l'esistenza di condizioni di rischio concreto dello sportello;
c) documentazione tecnica relativa all'installazione dei sistemi biometrici e di videosorveglianza adottati, dal quale risulti la conformita' dei medesimi alle condizioni indicate nel presente provvedimento. Dalla medesima devono evincersi:
le caratteristiche dell'impianto di ripresa (ad esempio, localizzazione della/e telecamera/e con l'indicazione delle caratteristiche tecniche);
le caratteristiche dell'impianto di raccolta del dato biometrico;
le caratteristiche del sistema informatico di gestione delle immagini e dei dati biometrici, con particolare riguardo alle fasi del processo crittografico;
l'indicazione del tempo massimo di conservazione dei dati;
d) copia dell'informativa resa alla clientela;
e) documentazione dalla quale si possano desumere le modalita' alternative di accesso alla struttura della banca.
Tutto cio' premesso, il Garante:
1. ai sensi dell'art. 154, comma 1, lettera c), del Codice prescrive a tutti i titolari del trattamento di adottare le misure necessarie indicate nel presente provvedimento al fine di rendere il trattamento conforme alle disposizioni vigenti;
2. individua nei termini di cui in motivazione, ai sensi dell'art. 24, comma 1, lettera g) del Codice, i casi nei quali il trattamento dei dati personali nell'ambito dei sistemi informativi oggetto del presente provvedimento puo' essere effettuato dagli istituti di credito, nei limiti e alle condizioni indicate, per perseguire legittimi interessi senza richiedere il consenso degli interessati;
3. dispone che copia del presente provvedimento sia trasmesso al Ministero della giustizia Ufficio pubblicazione leggi e decreti, per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 27 ottobre 2005

Il presidente: Pizzetti

Il relatore: Fortunato

Il segretario generale: Buttarelli

Allegato