SERVIZIO RELAZIONI ISTITUZIONALI

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Verifica preliminare (art. 17 del Codice) - 23 febbraio 2006 — Bollettino del n. 69/febbraio 2006, pag. 0

[doc. web n. 1251535]

Dati biometrici e Rfid nelle banche - 23 febbraio 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;

Esaminata la richiesta di verifica preliminare presentata da San Paolo Imi S.p.a. ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), relativa all'introduzione, in via sperimentale, di modalità di trattamento di dati personali biometrici e dell'utilizzo di una tessera-servizi che si avvale della tecnologia Rfid;

Visti gli atti d'ufficio;

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. Trattamento di dati personali dei clienti attraverso il servizio sperimentale denominato "*Service card*"

San Paolo Imi S.p.A. ha presentato al Garante una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice in relazione al progetto sperimentale *Filiale "High Tech"*.

In base ad esso, i clienti che lo richiedano verranno dotati di una smart card con microprocessore *Rfid* denominata *Service Card*, volta a facilitare la fruizione di taluni servizi rendendo immediatamente visibile sul terminale del personale operante presso la banca la "posizione" del cliente, e agevolando l'accesso diretto a talune aree dedicate (ad es.,

"chiosco banca diretta").

Nella *smart card* sarebbero memorizzate unicamente talune informazioni, non immediatamente correlabili al cliente (numero seriale precodificato della tessera, codice Abi della banca e codice del contratto di *Internet Banking*), conoscibili da parte del personale della banca all'atto di prestare servizi mediante la tecnologia Rfid (semplicemente accostando la "*service card*" ad un lettore). La service card non consentirebbe di tracciare la posizione geografica del detentore.

Inoltre, nel caso di operazioni bancarie poste in essere avvalendosi del sistema di *Internet banking* disponibile presso il "chiosco banca diretta" sito nella *Filiale "High Tech"*, verrebbe attribuita al cliente la facoltà di identificarsi, oltre che ricorrendo alle tradizionali credenziali di autenticazione (*Personal identification number-Pin*), anche previo procedimento di controllo biometrico dell'identità. I dati biometrici verrebbero conferiti facoltativamente. Resterebbe altresì attribuito alla libera scelta del cliente l'utilizzo di un codice numerico di identificazione personale, in luogo del sistema biometrico (*cfr. comunicazione San Paolo Imi S.p.A. del 14 novembre 2005, all. 1, punti 5 e 20*).

Il procedimento biometrico volto ad identificare il cliente sarebbe basato sulla previa rilevazione dell'impronta digitale dell'interessato, sulla successiva trasformazione della medesima in sede di *enrolment* in un codice numerico (tramite una procedura che si asserisce essere "irreversibile", denominata *one-way hashing*, che renderebbe impossibile, ad avviso della richiedente, risalire non solo all'immagine dell'impronta digitale, ma anche al *template* da questa generato) e sulla memorizzazione di quest'ultimo in un archivio centralizzato della banca. Il *template* così registrato verrebbe quindi utilizzato quale termine di paragone rispetto ai dati biometrici rilevati in occasione di ciascuna autenticazione da parte del cliente nell'ambito dei servizi resi disponibili nella *Filiale "High Tech"*. I dati biometrici dell'interessato, ove collimanti con quelli memorizzati nel database centralizzato, verrebbero dunque utilizzati per sostituire le credenziali di autenticazione più tradizionali.

2. Dati biometrici e disciplina di protezione dei dati personali: principi di liceità, finalità e pertinenza nel trattamento

La richiesta di verifica preliminare relativa all'utilizzo di dati biometrici riguarda un'ipotesi di trattamento di dati personali. Sia le impronte digitali, sia i dati biometrici da esse ricavati e successivamente utilizzati per verifiche e raffronti nelle procedure di autenticazione o di identificazione, sono informazioni personali riconducibili ai singoli interessati (art. 4, comma 1, lett. b), del Codice), alle quali trova applicazione la disciplina contenuta nel Codice (cfr. *Provv*. Garante 19 novembre 1999, in *Boll.* n. 10, p. 68, doc. web n. 42058; 21 luglio 2005, in *Boll.* n. 63, doc. web n. 1150679; 23 novembre 2005, in *Boll.* n. 66, doc. web n. 1202254; in merito v. pure Gruppo Art. 29, *Documento di lavoro sulla biometria-Wp80*, punto 3.1.).

La finalità perseguita dalla banca richiedente (titolare del trattamento), consistente nell'identificare i soggetti abilitati a svolgere attività negoziale presso aree della banca appositamente attrezzate ("chiosco banca diretta"), è lecita. Pur potendo, a tal fine, essere utilizzati dati biometrici –assicurando i medesimi, allo stato, un elevato grado di attendibilità nel procedimento di identificazione–, risulta sproporzionata, invece, la centralizzazione in un database delle informazioni personali (in forma di *template* ricavati dalla rilevazione delle impronte digitali) trattate nell'ambito del descritto procedimento di riconoscimento biometrico: in ossequio al principio di necessità (art. 3 del Codice), i sistemi informativi

devono essere infatti configurati in modo da ridurre al minimo l'utilizzazione di dati personali, e da escluderne il trattamento, quando le finalità perseguite nei singoli casi possono essere realizzate con altre modalità (in particolare, mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità).

Nella fattispecie sottoposta a verifica preliminare la banca, senza (aver la necessità di) creare un archivio centralizzato di impronte digitali o di *template*, e fatte salve le operazioni necessarie a generare il *template* in fase di *enrolment*, potrà avvalersi comunque di un sistema efficace di verifica e di identificazione biometrica, improntato però sulla lettura delle impronte digitali memorizzate sotto forma di *template* cifrato su uno strumento posto nell'esclusiva disponibilità del cliente (*smart card* o dispositivo analogo) –che ben potrebbe essere la stessa "*service card*"– in luogo della prospettata centralizzazione in un database.

Tale modalità di riconoscimento biometrico è parimenti idonea a garantire un adeguato livello di accuratezza in ordine all'accertamento dell'identità del detentore della smart card (il confronto delle impronte digitali con il *template* memorizzato sulla carta potrà essere realizzato, infatti, ricorrendo a procedure di *matching on card* o di *matching on device*), senza la costituzione di un archivio di informazioni personali –peraltro particolarmente delicate–, prevenendo così il rischio di eventuali utilizzi impropri o possibili abusi (in questo senso, v. *Provv*. Garante 23 novembre 2005, in http://www.garanteprivacy.it, doc. web n. 1202254).

3. Qualità dei dati e misure di sicurezza rispetto al trattamento dei dati biometrici

In attuazione dell'obbligo di adottare ogni necessaria misura di sicurezza, anche minima (art. 31 ss. e Allegato B al Codice), la banca resta obbligata a farsi rilasciare dall'installatore del sistema il previsto attestato di conformità, e a conservarlo presso la propria struttura (regola n. 25 dell'Allegato B al Codice).

Resta parimenti ferma, con particolare riguardo alla raccolta dei dati da parte degli incaricati operanti sotto la diretta autorità del responsabile del trattamento (che verrebbe individuato nel "*responsabile pro tempore della Direzione Macchina Operativa Integrata*": comunicazione San Paolo Imi del 14 novembre 2005, all. 1, punto 20), la necessità di designarli per iscritto, impartendo loro idonee istruzioni alle quali attenersi.

4. L'utilizzo della tecnologia Rfid

Non emergono, con riguardo alla "*service card*", profili di illiceità del trattamento. La tessera è sprovvista di informazioni immediatamente identificative (essendo la sola banca in grado di associarle al cliente). I dati personali in essa inseriti risultano pertinenti e non eccedenti, trattandosi di informazioni funzionali all'esecuzione delle operazioni bancarie. Anche in relazione alle modalità trasmissive delle informazioni mediante il sistema Rfid non risultano, allo stato, rischi specifici in relazione ai dati personali trattati: la tecnica utilizzata non caratterizza significativamente la modalità d'uso della tessera stessa rispetto alle tradizionali smart card, e la ridotta distanza operativa di lettura (non superiore a 2 centimetri) appare precludere l'acquisizione anche inconsapevole dei dati contenuti nella tessera da parte di soggetti estranei al trattamento.

Quale accorgimento aggiuntivo a garanzia dell'interessato (cfr. art. 17 del Codice), la banca dovrà attuare, dandone comunicazione a questa Autorità entro il 20 aprile 2006, le misure idonee affinché vengano inibite immediatamente, in modo automatico, tutte le funzioni

connesse all'uso della carta in caso di smarrimento o furto della "*service card*".

Va rilevato che, stante il quadro emergente dal progetto, il personale della banca può comunque richiedere l'esibizione di documenti d'identità in corrispondenza dell'esecuzione di operazioni bancarie (cfr. in merito la decisione del Garante del 27 ottobre 2005, in http://www.garanteprivacy.it, doc. web n. 1189435).

5. Informativa, consenso e notificazione del trattamento

L'informativa che la banca ha predisposto (acquisita agli atti) include gli elementi previsti dalla legge (art. 13 del Codice).
Si constata altresì che la banca raccoglie uno specifico consenso degli interessati (sia per i trattamenti effettuati mediante la *service card*, sia per l'utilizzo di dati biometrici) e che provvederà a notificare al Garante il trattamento dei dati biometrici prima che abbiano inizio le operazioni di trattamento (art. 37, comma 1, lett. a), del Codice).

6. Considerazioni conclusive

I trattamenti di dati personali oggetto della presente verifica preliminare potranno essere effettuati nel rispetto delle misure e degli accorgimenti riassunti nel seguente dispositivo.

Esaurita la fase sperimentale realizzata presso la "*Filiale High Tech*", San Paolo Imi S.p.A. dovrà darne comunicazione a questa Autorità indicandone gli esiti per quanto attiene i profili di protezione dei dati personali. Valutata da parte del Garante l'adeguatezza degli accorgimenti e delle misure adottati e riscontrato, sempre da parte dell'Autorità, che non si siano manifestate controindicazioni per i diritti degli interessati, San Paolo Imi S.p.a. potrà chiedere di attivare analoghi sistemi presso altre dipendenze senza che sia necessario sottoporli a nuova verifica preliminare, sempreché ne restino inalterate le caratteristiche.

TUTTO CIÒ PREMESSO IL GARANTE

prescrive al titolare del trattamento, ai sensi degli artt. 17 e 154, comma 1, lett. c) del Codice, al fine di conformarsi alle disposizioni vigenti, di adottare le misure e gli accorgimenti a garanzia degli interessati nei termini di cui in motivazione, dandone comunicazione a questa Autorità entro il 20 aprile 2006, ed in particolare:

a) in relazione a quanto indicato al punto 2 di cui in motivazione, predisporre un sistema di verifica basato sul confronto tra le impronte rilevate ad ogni accesso al sistema e il *template* memorizzato e cifrato su un supporto che resti nell'esclusiva disponibilità degli interessati, senza creare un archivio centralizzato di *template* tratti dalle impronte digitali;

b) in relazione a quanto indicato al punto 4, attuare le misure idonee affinché vengano immediatamente inibite, in modo automatico, tutte le funzioni connesse all'uso della "*service card*", in caso di smarrimento o furto.

Roma, 23 febbraio 2006

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli