SERVIZIO RELAZIONI ISTITUZIONALI

[doc. web n. 1306098]

Uso della biometria per identificazione del personale nelle banche - 15 giugno 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 dalla Cassa di risparmio di Ferrara S.p.a. ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

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. Mauro Paissan;

PREMESSO

1. Trattamento di dati personali biometrici di personale autorizzato per finalità di sicurezza, riservatezza e protezione dei beni in una particolare area della sede dell'istituto bancario

La Cassa di risparmio di Ferrara S.p.a. ha presentato una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, relativa al trattamento di dati biometrici di un numero ristretto di soggetti (complessivamente non superiore a trenta unità, comprendenti amministratori e dipendenti della banca) autorizzati all'accesso ad un'area particolare della sede nella quale sono situati gli uffici della presidenza e la direzione generale della banca. Si tratta, segnatamente, di un piano dell'edificio (non aperto al pubblico e privo di sportelli e uffici operativi) al quale allo stato si accede, previo riconoscimento da parte del personale di portineria, cui è rimesso il compito di azionare l'arresto degli ascensori al piano sopra indicato.

Le finalità di tale sistema sono di garantire la sicurezza del personale della direzione (evitando che persone estranee accedano a tale area: come accaduto in passato: cfr. richiesta

di verifica preliminare), la riservatezza di documenti e fascicoli, nonché la protezione di opere d'arte ivi custodite.

Il sistema di riconoscimento, isolato e non comunicante con altri, non verrebbe utilizzato per ulteriori finalità; la sua adozione consentirebbe ai soggetti autorizzati –che su base volontaria e previa informativa intendano avvalersene– di salire al piano senza l'intervento del personale di portineria, utilizzando i menzionati ascensori dotati al proprio interno di un apposito lettore delle impronte digitali. Una volta raccolta, l'immagine dell'impronta dell'ultima falange del dito destro o sinistro verrebbe trasformata in un algoritmo matematico, successivamente confrontato con il modello registrato in un database dedicato, nel quale sarebbero centralizzati i *template* dei soggetti autorizzati.

A giudizio della banca non sarebbe possibile ricostruire il dato biometrico originario, tenendo conto del fatto che il codice numerico generato verrebbe criptato.

Le informazioni relative agli accessi al piano (data ed ora) verrebbero conservate per un periodo di sette giorni e, con cadenza semestrale, verrebbero aggiornati i nominativi dei soggetti autorizzati ad avvalersi della descritta procedura (cfr. comunicazioni della banca del 27 dicembre 2005 e del 20 marzo 2006).

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

2.1. Il caso sottoposto alla verifica preliminare di questa Autorità integra un'ipotesi di trattamento di dati personali. Sia le impronte digitali, sia i dati 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*. 19 novembre 1999, in Boll. n. 10, p. 68, doc. web n. 42058 e 21 luglio 2005, in *Boll.* n. 63, doc. web n. 1150679; in merito v. pure il documento di lavoro sulla biometria del Gruppo art. 29, direttiva n. 95/46/Ce -wp80-, punto 3.1.).

L'uso generalizzato e incontrollato di dati biometrici, specie se ricavati dalle impronte digitali, non è in linea di principio lecito. Tali dati, per la loro peculiare natura, richiedono l'adozione di elevate cautele al fine di prevenire possibili pregiudizi ai danni degli interessati, con particolare riguardo a condotte illecite che determinino l'abusiva "ricostruzione" dell'impronta partendo dal *template* e la sua ulteriore "utilizzazione" all'insaputa degli stessi.

L'utilizzo di dati biometrici può essere, quindi, giustificato in casi particolari, tenuto conto delle finalità e del contesto in cui essi sono trattati e, in relazione ai luoghi di lavoro, per presidiare accessi ad "aree sensibili", considerata la natura delle attività ivi svolte (si pensi, ad esempio, a processi produttivi pericolosi o sottoposti a segreti, di varia natura: cfr. *Provv*. 23 novembre 2005, in *http://www.garanteprivacy.it*, doc. web n. 1202254) o in ragione della documentazione o dei beni ivi custoditi (quali, documenti segreti o riservati, oggetti di valore, etc.).

2.2. Nella fattispecie in esame, la finalità perseguita dalla banca è, in termini generali, lecita. La centralizzazione in un *database* delle informazioni personali (in forma di *template*)

trattate nell'ambito del descritto procedimento di riconoscimento biometrico risulta, tuttavia, sproporzionata e non necessaria, atteso che i sistemi informativi devono essere configurati in modo da ridurre al minimo l'utilizzazione di dati personali e da escluderne il trattamento, quando le finalità perseguite possono essere realizzate con modalità tali da permettere di identificare l'interessato solo in caso di necessità (artt. 3 e 11 del Codice).

In luogo della prospettata centralizzazione, deve ritenersi adeguato e sufficiente avvalersi di un sistema efficace di verifica e di identificazione biometrica basato sulla lettura delle impronte digitali memorizzate, sotto forma di template cifrato, su un supporto posto nell'esclusiva disponibilità dell'interessato (*smart card* o dispositivo analogo) e privo di indicazioni nominative a quest'ultimo riferibili (quale un codice individuale).

Tale modalità di riconoscimento, infatti, è parimenti idonea ad assicurare che possano accedere all'area riservata solo coloro che, previamente autorizzati, decidano su base volontaria di avvalersi della *smart card* –in relazione alla quale il confronto delle impronte digitali con il template memorizzato sulla carta potrà essere realizzato ricorrendo a procedure di *matching on card* o di *matching on device*–; è possibile così evitare la costituzione di un archivio di dati biometrici (come detto particolarmente delicati), prevenendo il rischio di eventuali utilizzi impropri dei dati o di possibili abusi (in questo senso, v. *Provv*. 23 novembre 2005, in *http://www.garanteprivacy.it*, doc. web n. 1202254).

3. Informativa agli interessati e notificazione del trattamento
L'informativa che la banca dovrà rendere rispetto al trattamento che intende porre in essere deve risultare completa degli elementi previsti dal Codice (art. 13).

In particolare, tenuto conto del diverso sistema suscettibile di impiego secondo l'avviso di questa Autorità (indicato al punto 2.2.), l'informativa (in atti) predisposta dalla banca –nella quale è, peraltro, chiaramente rappresentato il carattere volontario del ricorso al sistema di riconoscimento biometrico–, dovrà essere integrata con riguardo al profilo relativo alle modalità del trattamento.

4. Misure ed accorgimenti

4.1. La banca resta tenuta a designare per iscritto tutti i soggetti che effettuino operazioni di trattamento dei dati (con particolare riguardo alla registrazione dei *template* sui menzionati supporti), quali incaricati o, eventualmente, responsabili delle operazioni di trattamento, impartendo loro idonee istruzioni alle quali attenersi.

Tali istruzioni dovranno riguardare anche le misure da adottare in caso di eventuale perdita e sottrazione dei dispositivi, nonché al ciclo di utilizzazione dei dispositivi di autenticazione e le procedure interne per verificare il sistema ed aggiornare, ove necessario, i dispositivi affidati.

4.2. In attuazione dell'obbligo di adottare ogni misura anche minima di sicurezza prescritta dal Codice (art. 31 ss. e Allegato B), la banca dovrà farsi rilasciare dall'installatore del sistema il prescritto attestato di conformità e conservarlo presso la propria struttura (regola n. 25 del Disciplinare tecnico in materia di misure minime di sicurezza - Allegato "B" al Codice).

4.3. La società dovrà notificare al Garante il trattamento dei dati biometrici prima che

abbiano inizio le operazioni di trattamento (art. 37, comma 1, lett. a), del Codice).

5. Conservazione dei dati

I dati personali necessari alla realizzazione del *template* potranno essere trattati esclusivamente durante tale fase (c.d. *enrollment*).

I dati relativi agli orari di accesso dei soggetti che utilizzeranno il descritto sistema di riconoscimento biometrico, accessibili al personale preposto al rispetto delle misure di sicurezza all'interno della banca e per l'esclusiva finalità dell'osservanza delle medesime, potranno essere conservati per il tempo massimo di sette giorni, assicurando, oltre il predetto arco temporale meccanismi di cancellazione automatica dei dati. Tale intervallo temporale, peraltro indicato nella richiesta formulata dalla banca, appare ragionevole tenendo conto della documentazione e dei beni custoditi nell'area riservata (che si intendono con tale sistema proteggere), la cui sottrazione potrebbe essere scoperta a distanza di tempo.

TUTTO CIÒ PREMESSO IL GARANTE

prescrive al titolare del trattamento, ai sensi degli artt. 17 e 154, comma 1, lett. c), del Codice, di adottare le misure e gli accorgimenti a garanzia degli interessati nei termini di cui in motivazione, ed in particolare:

1. di predisporre un sistema di riconoscimento basato sul confronto tra le impronte rilevate ad ogni accesso all'area riservata e il *template* memorizzato e cifrato su un supporto che resti nell'esclusiva disponibilità degli interessati, senza creare a tal fine un archivio centralizzato di impronte digitali o di *template* individuali (punto 2.2.);
2. di riformulare l'informativa resa agli interessati, con riferimento alle modalità impiegate nel trattamento, descritte al punto 2.2 del presente provvedimento (punto 3.);
3. di conservare i dati relativi agli orari di accesso all'area riservata per il tempo massimo di sette giorni (punto 5).

Roma, 15 giugno 2006

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli