

Prov. Gar. Prot. Dati Pers. 28 settembre 2001
Rilevazioni biometriche – Rilevazioni biometriche in banca

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice-presidente, del prof. Gaetano Rasi e del dottor Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Viste le note della Banca CRT-Cassa di Risparmio di Torino del 12 aprile 2001 e della Veneto Banca S.c.a.r.l. del 14 marzo 2001;

VISTI gli atti d'ufficio;

VISTE le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il Prof. Gaetano Rasi;

PREMESSO:

1. Il Garante ha già esaminato, anche con recenti provvedimenti, il tema dell'installazione all'entrata degli istituti bancari dei sistemi di rilevazione delle impronte digitali degli utenti, eventualmente associate ad immagini.

L'Autorità ha constatato che l'utilizzo generalizzato ed indiscriminato di tali sistemi non è consentito in quanto viola il principio di proporzionalità tra gli strumenti impiegati e le finalità prospettate (art. 9 legge n. 675/1996), perseguibili attraverso altri mezzi che comportano minori problemi per la tutela dei diritti e della dignità delle persone interessate.

Un'attività indifferenziata di raccolta di dati significativi quali quelli relativi alle impronte digitali, imposta a tutti coloro -clienti o meno- che entrano in un istituto bancario non può ritenersi legittimata da una generica esigenza di sicurezza.

In mancanza di specifici elementi che evidenzino una concreta situazione di rischio tale attività si tradurrebbe in un sacrificio sproporzionato della sfera di libertà e della dignità delle persone interessate. Ciò anche in considerazione della particolare natura delle informazioni raccolte.

Le impronte digitali presuppongono infatti specifiche valutazioni rispetto a differenti rilevazioni di natura biometrica. La cautela e la selettività sono tanto più necessarie se si considera il rischio di ipotetiche utilizzazioni abusive contrastabili ricorrendo a più avanzati sistemi tecnologici.

Va inoltre tenuto conto del bilanciamento già operato nel nostro ordinamento riguardo alla raccolta di questo genere di informazioni da parte di soggetti pubblici, in quanto la raccolta delle impronte digitali da parte di organi di polizia o giudiziari è basata su apposite previsioni normative che delimitano la rilevazione nei confronti di persone pericolose o sospette, o di coloro che non sono in grado o si rifiutano di provare la propria identità, oppure in caso di identificazione di un indagato o di detenuti ed internati all'ingresso di un istituto penitenziario (art. 7 r.d. n. 635/1940; artt. 349, comma 2, c.p.p. e 23/26 d.P.R. n. 230/2000).

Questo quadro normativo evidenzia la necessità di una base legislativa che

regoli in modo equilibrato la materia e tenga conto dei diritti fondamentali delle persone interessate. Non a caso tale base è stata prevista - peraltro in termini insufficienti - per la possibile inclusione di dati biometrici all'interno della c.d. carta di identità elettronica (tema sul quale il Garante si è pronunciato con alcuni provvedimenti riportati nel Bollettino dell'Autorità e nel proprio sito web www.garanteprivacy.it).

Una ulteriore conferma deriva anche dalla Raccomandazione del Consiglio d'Europa N.R (87) 15 in materia di dati utilizzati a fini di pubblica sicurezza, che l'Italia si è impegnata ad attuare, la quale consente la raccolta di dati mediante dispositivi tecnici di sorveglianza o altri mezzi automatizzati solo se prevista da disposizioni specifiche (punto 2.3).

Sulla base di detti principi i sistemi di rilevazione delle impronte digitali in precedenza installati presso alcuni istituti bancari oggetto di segnalazioni del Garante sono stati quindi disattivati.

2. Altri istituti bancari chiedono ora al Garante di poter utilizzare presso propri sportelli, in relazione a specifiche situazioni di rischio, sistemi di temporanea acquisizione cifrata delle impronte eventualmente associati ad immagini. A tali dati cifrati potrebbero accedere successivamente soltanto organi giudiziari o di polizia.

L'Associazione bancaria italiana (ABI) ha poi inviato una nota rappresentando alcune esigenze connesse, in particolare, all'imminente introduzione della moneta unica e alla conseguente disponibilità presso gli istituti bancari, negli ultimi mesi del 2001 e nei primi mesi del 2002, di ingenti quantitativi di denaro contante.

Si pone quindi l'esigenza di valutare se, in mancanza di una necessaria base legislativa, sia al momento possibile considerare lecita detta installazione, temporaneamente e in considerazione delle eccezionali circostanze determinatesi.

L'Autorità è consapevole dell'esigenza di sicurezza che si pone in particolari situazioni ed è parimenti consapevole della specificità che la realtà bancaria pone rispetto ad altri soggetti privati che potrebbero presentare analoghe istanze.

Nel confermare quindi l'orientamento manifestato anche con recenti provvedimenti ritiene possibile svilupparne alcuni principi, con particolare riguardo all'individuazione delle particolari circostanze di rischio menzionate nelle decisioni già adottate.

Si tratta, come si è accennato, di soluzioni temporanee e prodromiche ad un futuro intervento legislativo che disciplini compiutamente la materia. Tali soluzioni dovranno rispettare alcune imprescindibili garanzie, in mancanza delle quali l'attività di rilevazione in questione non è ritenuta lecita.

3. L'utilizzazione dei sistemi di rilevazione cifrata delle impronte digitali non può essere anzitutto generalizzata, ma deve essere riferita a situazioni di concreto rischio riconducibili a circostanze obiettive, valutate dall'istituto bancario con particolare cautela, anche sulla base di precedenti eventi e di concordanti valutazioni da parte dei locali e competenti organi in materia di tutela dell'ordine e della sicurezza pubblica.

Per rendere possibile una valutazione di insieme del fenomeno è poi essenziale che gli istituti bancari diano comunicazione circa i sistemi installati

al locale comitato provinciale per l'ordine e la sicurezza pubblica e all'associazione nazionale di categoria.

In relazione all'interesse manifestato al problema dall'ABI e da alcune prefetture, il Garante invita pertanto questi ultimi a fornire ogni utile collaborazione al riguardo.

4. La rilevazione cifrata delle impronte digitali non può dar luogo ad alcuna "schedatura" da parte degli istituti di credito, né può comportare altrimenti una privazione della libertà degli utenti degli sportelli bancari.

L'accesso agli sportelli bancari tramite i sistemi di rilevazione installati deve avvenire su base volontaria e consensuale (cfr. artt. 11 e 12 legge n. 675/1996), abbinando il sistema di rilevazione ai comuni dispositivi di ingresso già installati, evitando così all'utente l'uso di meccanismi complicati ed ulteriori oltre quelli già oggi utilizzati (in particolare l'istituto deve adoperarsi affinché la rilevazione dell'impronta avvenga, con un'unica operazione, all'atto di premere l'ordinario pulsante previsto per l'accesso).

Deve essere poi predisposto un meccanismo che, in caso di indisponibilità dell'utente, permetta a quest'ultimo di accedere comunque all'istituto bancario, con eventuale adozione -nei soli casi necessari- di misure di cautela rimesse alla ragionevole valutazione dei responsabili della filiale (es.: richiesta di esibizione di un documento per casi di ingresso di persone sospette).

Deve ritenersi precluso ogni infondato comportamento vessatorio nei confronti di coloro che al momento dell'accesso alla filiale bancaria non ritengono di acconsentire alla rilevazione dell'impronta.

5. Va tenuto conto anche dei seguenti principi:

- a) informativa agli interessati

Si devono fornire all'ingresso degli istituti indicazioni chiare, anche se sintetiche, che avvertano gli utenti della presenza di sistemi di acquisizione cifrata di impronte digitali e dell'eventuale associazione contemporanea con un'immagine, fornendo le informazioni necessarie ai sensi dell'art. 10 della legge n. 675/1996.

Si potrà fornire l'informativa anche attraverso messaggi brevi e in stile colloquiale, eventualmente uniti a simboli, sulla falsariga dell'informativa già suggerita dal Garante in materia di videosorveglianza (es.: *"La banca rileva l'impronta digitale e l'immagine dei visitatori come misura precauzionale per l'eventuale commissione di reati. I dati sono cifrati e accessibili solo all'autorità giudiziaria o di polizia e sono cancellati in breve tempo. Il personale non vi accede. Gli interessati possono esercitare i propri diritti (art. 13 l. 31 dicembre 1996, n. 675) rivolgendosi al servizio...E' possibile entrare con altre modalità nei locali rivolgendosi al personale"*).

L'informativa dovrà essere apposita e collocata all'ingresso degli istituti.

- b) misure di sicurezza

Occorre adottare misure di sicurezza corrispondenti ai parametri previsti dall'art. 15, comma 1, della legge n. 675/1996, conformi alle misure minime di cui al comma 2 del medesimo articolo e al d.P.R. n. 318/1999 in particolare per quanto riguarda la custodia delle "chiavi" di accesso al sistema e ai dati.

I sistemi di rilevazione devono offrire una rigorosa garanzia di affidabilità ed integrità dei dati, anche sulla base di eventuali certificazioni od omologazioni dei dispositivi.

Le informazioni relative alle impronte e alle eventuali immagini devono essere rigorosamente protette da sistemi di cifratura automatica sin dal momento della loro rilevazione. L'eventuale associazione alle immagini non deve essere possibile se non dopo l'eventuale decrittazione.

c) accesso ai dati

Soltanto l'autorità giudiziaria o di polizia, e con riferimento a specifiche attività investigative connesse alla commissione di reati, può decifrare ed avere eventuale accesso alle informazioni non nominative raccolte con i sistemi di rilevazione.

Il personale anche esterno alla banca preposto all'utilizzo e alla manutenzione delle apparecchiature non deve poter avere in alcun modo accesso "in chiaro" alle informazioni cifrate (immagini ed impronte).

d) conservazione

I dati cifrati relativi alle impronte e alle eventuali immagini devono essere conservati in *file* giornalieri per un periodo non superiore a una settimana.

Devono essere predisposti meccanismi di integrale cancellazione automatica delle informazioni allo scadere del termine previsto. Resta ferma, durante il predetto periodo, la possibilità per gli organi giudiziari o di polizia di acquisirle e conservarle agli atti del procedimento.

Non può ritenersi consentito alcun sistema di indicizzazione dei dati o di creazione di ulteriori banche dati, come pure di sistemi di riconoscimento facciale.

e) notificazione

Nei casi in cui la legge impone la notificazione al Garante dei trattamenti di dati personali (art. 7 legge n. 675/1996), fra le modalità di trattamento utilizzate dovrà ovviamente indicarsi anche la raccolta di informazioni mediante sistemi di acquisizione cifrata delle impronte digitali eventualmente associate ad immagini.

6. Il Garante si riserva di adottare ulteriori iniziative in materia e delibera di inviare copia del presente provvedimento anche all'ABI e al Ministero dell'interno, per l'auspicata collaborazione in ordine a quanto sopra indicato.

TUTTO CIO' PREMESSO IL GARANTE:

- segnala agli istituti bancari istanti, ai sensi dell'art. 31, comma 1, lett. c), della legge n. 675/1996, la necessità di conformare il trattamento dei dati ai principi della legge n. 675/1996 e ai criteri specificamente richiamati nel presente provvedimento.

Roma, 28 settembre 2001

IL PRESIDENTE
Rodotà
IL RELATORE
Rasi
IL SEGRETARIO GENERALE
Buttarelli