

15 aprile 2003 0:00

BANCA: IMPRONTE DIGITALI?

di Katia Moscano

Vediamo come il Garante per la Privacy e' intervenuto su questo argomento, in tre momenti diversi e successivi.

Inizialmente c'e' stato un comunicato stampa del luglio 2000, in riferimento alla notizia apparsa su di un organo di informazione sull'utilizzo di sistemi di rilevazione delle impronte digitali all'ingresso di un istituto di credito. In quell'occasione, l'Autorita' Garante per la protezione dei dati personali precisava che il caso era stato segnalato all'ufficio di sua competenza e che erano stati avviati degli accertamenti per verificare se il trattamento dei dati si svolgeva secondo i presupposti di liceita' e di correttezza previsti dalla legge n.675/1996.

Il Garante non rilascio' in merito alcun assenso, autorizzazione o parere, anche perche' la legge sulla privacy non prevede la necessita' di autorizzazioni a riguardo.

La legge, pero', impone che ogni trattamento dei dati personali sia svolto nel rispetto di precise cautele e garanzie sostanziali a tutela degli interessati.

Queste garanzie riguardano la trasparenza nell'utilizzo di questi sistemi, e dunque la dovuta informazione ai clienti, nonche' la previsione di specifiche misure per quanto concerne le finalita' perseguite, il trattamento delle informazioni rilevate, la limitata durata della loro conservazione, la sicurezza contro l'accesso illecito, l'individuazione del personale addetto al trattamento di questi dati.

Secondo comunicato stampa del Garante del dicembre 2000.

In questo caso il Garante ha stabilito che:

l'utilizzo di sistemi per una indiscriminata rilevazione delle impronte digitali all'ingresso delle banche e' sproporzionato rispetto a generiche esigenze di sicurezza che si intendano perseguire, gia' sufficientemente assicurate da altri sistemi di controllo meno lesivi della dignita' della persona.

Questo intervento del Garante fu richiesto da alcuni cittadini, i quali avevano segnalato che in una filiale di una banca erano stati installati due diversi sistemi di controllo degli ingressi e della permanenza dei clienti nei locali dell'istituto, sia attraverso la ripresa di immagini, sia mediante il rilevamento delle impronte digitali.

L'Autorita' ha chiesto chiarimenti alla banca circa le modalita' con cui venivano raccolti e utilizzati i dati, il periodo di conservazione, se trasmessi a terzi e alle autorita' pubbliche e dopo quanto tempo fossero cancellati.

Dalle indagini risulto' che per entrambi i sistemi non veniva fornita adeguata informativa ai clienti sulla presenza degli stessi, sull'uso delle informazioni raccolte e sui relativi diritti.

Non veniva, inoltre, posta adeguata attenzione sul collegamento tra l'immagine e le impronte rilevate.

Dunque l'Autorita' imponeva alla banca il divieto di utilizzare strumenti di rilevazione delle impronte digitali, sottolineando che la raccolta differenziata di dati significativi, quali le impronte digitali associate alle immagini, imposta a tutti coloro che entrano in una banca, siano essi clienti o meno, non puo' ritenersi di per se' legittimata da una generica esigenza di sicurezza, se non accompagnata da elementi che evidenzino una concreta situazione di rischio.

Infatti, in questo modo viene violato il principio della proporzionalita' tra almeno uno dei mezzi di identificazione impiegati e le finalita' perseguite.

Questa duplice raccolta di informazioni impone un sacrificio sproporzionato della sfera delle liberta' delle persone che possono legittimamente lamentare un rilevante pregiudizio della propria dignita' personale.

L'Autorita' ha invitato, inoltre, l'istituto a rivedere l'informativa ai clienti sui sistemi video, specificando gli scopi per i quali questi vengono impiegati, il periodo entro il quale le immagini sono cancellate, ecc.

Provvedimento del Garante -1 ottobre 2001- sull'argomento. In questo caso l'Autorita' Garante e' intervenuta per stabilire le prime rigorose regole in base alle quali, all'ingresso degli istituti bancari, puo' essere consentita l'installazione di sistemi di rilevazione cifrata che, in caso di necessita' permetta la lettura delle impronte digitali. Il provvedimento, sollecitato da alcuni istituti sulla base di istanze sindacali, si e' reso necessario in relazione alle specifiche esigenze di sicurezza di un settore a rischio.

L'Autorita' ha valutato entro quali limiti possa considerarsi lecita, nell'ambito della realta' bancaria, l'installazione di sistemi di acquisizione criptata delle impronte digitali, e quali devono essere le imprescindibili garanzie da assicurare per il rispetto dei diritti fondamentali delle persone.

La rilevazione delle impronte "esplicitamente", rimane sempre esclusivita' degli organi di polizia e giudiziari.

- 1) L'utilizzazione dei sistemi di rilevazione cifrata delle impronte digitali deve essere riferita a situazioni di rischio, valutate dall'istituto bancario anche sulla base di concordanti valutazioni da parte dei locali organi competenti per l'ordine e la sicurezza;
- 2) la rilevazione delle impronte non puo' dar luogo ad alcuna schedatura da parte degli istituti di credito e quindi non potranno costituire alcuna banca dati con le informazioni raccolte. L'accesso dei clienti e non agli sportelli, deve avvenire volontariamente e consensualmente: in caso di indisponibilita' dell'utente a sottoporsi alla rilevazione criptata, dovra' essere lasciata ai responsabili delle filiali la valutazione di far accedere comunque l'utente dentro l'istituto con eventuali ragionevoli cautele, astenendosi, pero', da qualsiasi comportamento vessatorio nei suoi confronti;
- 3) le informazioni relative alle impronte devono essere rigorosamente protette da sistemi di cifratura automatica sin dal momento della acquisizione. Non saranno dunque, immediatamente riconducibili a persone determinate e l'eventuale associazione alle immagini rilevate con telecamere, potra' avvenire solo dopo la decriptazione;
- 4) soltanto l'autorita' giudiziaria o di polizia, e solo nell'ambito nelle indagini connesse alla commissione di reati, potra' decifrare ed avere accesso alle informazioni. Il personale della banca non potra' avere, in alcun modo, accesso "in chiaro" alle informazioni cifrate;
- 5) i dati cifrati devono essere integralmente cancellati dopo una settimana;
- 6) gli istituti devono fornire all'ingresso indicazioni chiare che avvertano gli utenti della presenza dei sistemi di rilevazione e della possibilita' di accedere in modo diverso nei locali;
- 7) non e' consentito alcun sistema di indicizzazione dei dati o di riconoscimento facciale.

Questo provvedimento e' stato trasmesso all'Abi e al Ministero dell'Interno.