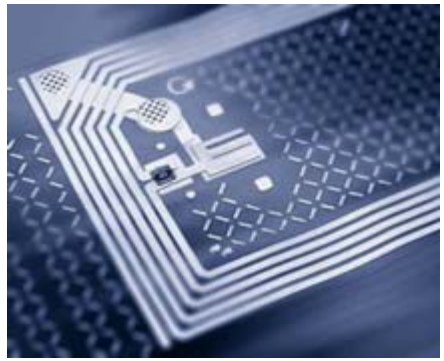
Le nuove potenzialità dei sistemi Rfid associati a dati biometrici: necessità e limiti



Michele Iaselli (ANDIP)

Firenze, 18 maggio 2007

Alcuni Istituti bancari hanno lanciato un progetto sperimentale denominato "Filiale High Tech" che consiste nel fornire ai clienti che lo richiederanno una smart card che sarà dotata di un microprocessore a radiofrequenza (Rfid), in cui saranno memorizzati numero della tessera e coordinate bancarie e verrà anche inserito, sempre a richiesta del cliente, il codice numerico di una impronta digitale.

Tale sistema consentirà al cliente di identificarsi, sostituendo in tal modo le tradizionali credenziali di autenticazione, cioè il PIN (Personal Identification Number) con il controllo biometrico.

Con l'inserimento di entrambe le tecnologie, la smart card passata su un lettore consentirà da una parte al personale preposto agli sportelli di conoscere immediatamente la "posizione" del cliente attraverso il chip a radiofrequenza e, dall'altra, permetterà al cliente stesso di effettuare operazioni mediante servizi self service e di banking on line presso talune aree dedicate, come ad esempio un "chiosco elettronico".

L’Autorità Garante per la protezione dei dati personali interpellata circa la legittimità di tale sistema ha adottato, in sede di verifica preliminare, una decisione favorevole alla utilizzazione della smart card prescrivendo però una serie di misure e garanzie a tutela dei dati.

Tali misure sono:

- la previsione di un sistema che preveda la memorizzazione dei codici numerici delle impronte su una smart card che deve rimanere nell'esclusiva disponibilità del cliente;
- il divieto di creare un archivio centralizzato delle impronte digitali della clientela, anche se cifrate;
- la necessità di richiedere uno specifico consenso da parte della clientela;
- la predisposizione di idonee misure per consentire l'immediata ed automatica disattivazione di tutte le funzioni della smart card in caso di smarrimento o di furto.

Inoltre ai clienti che non intendono avvalersi di questo nuovo sistema, dovrà essere comunque garantito l'accesso agli stessi servizi attraverso i tradizionali sistemi di autenticazione.

Il progetto "Filiale High Tech" risulta particolarmente interessante per la specifica implementazione di due tecnologie tra le più innovative degli ultimi tempi: RFID e biometria.

Rfid è un acronimo (Radio Frequency ID Devices) con cui si indicano dispositivi microscopici simili a microchip contenenti un identificativo (ad esempio, un numero di serie), che è possibile riconoscere attraverso un lettore compatibile funzionante in radiofrequenza.

Tali tecnologie si fondano sull'utilizzo di micro-processori che, collegati ad un'antenna ed impiegati come etichette di riconoscimento (*cd. etichette intelligenti*), sono in grado di trasmettere –attraverso onde radio– segnali leggibili da appositi lettori dotati di un'antenna di attivazione/ricezione.

La *Rfid* rappresenta uno strumento utile in numerosi settori e per diverse finalità: essa può essere impiegata, ad esempio, per il “tracciamento” di singole unità di prodotto nella catena di distribuzione dell’industria; per la prevenzione di furti e di contraffazioni dei prodotti; per garantire una maggiore rapidità nelle operazioni commerciali; per il controllo degli accessi ad aree riservate.

Ma attraverso le cd. “etichette intelligenti” si possono trattare, anche senza che l’interessato ne sia a conoscenza, innumerevoli dati personali che lo riguardano, compresi quelli di natura sensibile; raccogliere dati sulle abitudini del medesimo ai fini di profilazione attraverso l’aggregazione con altre informazioni di carattere personale; verificare prodotti (vestiti, accessori, medicine, ecc.) indossati o trasportati; tracciare i percorsi effettuati.

In questo settore il problema privacy sta diventando molto delicato perché tale tecnologia presenta enormi potenzialità: in prospettiva, anche in vista dell'ulteriore sviluppo tecnologico, dell'abbattimento dei costi di produzione, della possibilità di integrazione con altre infrastrutture di rete (telefonia, Internet, ecc.), le tecniche di identificazione via radio-frequenza potranno avere un impiego sempre maggiore e nei più diversi settori.

Occorre tenere altresì presente che più gravi pericoli per gli interessati possono derivare dal prevedibile incremento della potenza dei sistemi di *Rfid* (i quali potrebbero rendere fattibile una “lettura” delle etichette a maggiori distanze) nonché – specie in ragione dell’adozione di *standard* tecnici comuni – dalla possibilità che terzi non autorizzati “leggano” i contenuti delle etichette o intervengano sugli stessi (mediante, ad esempio, “riscrittura”).

Per questi motivi il Garante ha svolto una prima attività di approfondimento della materia (provvedimento generale del 9 marzo 2005) rivolgendo l’attenzione al possibile impatto che le tecniche di identificazione via radio possono già avere sulle condizioni di esercizio delle libertà delle persone e alle problematiche che la loro introduzione è destinata a sollevare relativamente all’applicazione della normativa sulla tutela dei dati personali.

Del resto è notizia recente che l'obiettivo perseguito dalla Commissione europea attraverso una recente Comunicazione diffusa all'esito di una consultazione pubblica conclusasi nel 2006 è proprio una politica europea per i sistemi Rfid che coniughi l'esigenza di sfruttare le potenzialità di questa tecnologia con l'attenzione alla tutela della privacy ed ai possibili rischi per la salute e l'ambiente.

I sistemi biometrici

Le tecnologie biometriche, consentono, mediante l'uso di specifici software e apparecchiature informatiche, il riconoscimento di un individuo attraverso dati fisici ricavati dall'analisi delle impronte digitali, della morfologia facciale e dal riconoscimento palmare.

Si tratta della ricerca più avanzata in tema di sicurezza degli accessi informatici. Alcune caratteristiche fisiche dell'utente autorizzato all'accesso, vengono memorizzate dal computer e confrontate con quelle della persona che accede.

Tra i sistemi biometrici si ricordano:

1. *le impronte digitali e le impronte palmari*;
2. *il riconoscimento della voce* (difettoso in caso di malattie da raffreddamento);
3. *il reticolo venoso della retina dell'occhio*;
4. *il controllo dinamico della firma* (con riferimento anche alla sua velocità di esecuzione).

Di fronte alla rapida ascesa di tali metodologie il Garante sta assumendo un atteggiamento particolarmente rigido in quanto spesso le finalità di identificazione, sorveglianza, sicurezza delle transazioni non possono giustificare qualsiasi utilizzazione del corpo umano resa possibile dall'innovazione tecnologica.

Vanno garantiti sempre il rispetto della dignità della persona, il rispetto dell’identità personale, il rispetto dei principi di finalità e di proporzionalità ed infine la necessaria attenzione per gli effetti cosiddetti imprevisti o indesiderati e che, invece, spesso sono conseguenze determinate da analisi incomplete o troppo interessate delle tecnologie alle quali si intende ricorrere.

Ma ciò che più preoccupa è che il problema della protezione dell'identità dai suoi possibili "furti", già imponente nel settore del commercio elettronico, rischia di assumere aspetti preoccupanti con l'utilizzo della biometria.

L’Autorità Garante già è intervenuta, con un provvedimento del 28 settembre 2001, per stabilire le prime rigorose regole in base alle quali, all’ingresso degli istituti bancari, può essere consentita l’installazione di sistemi di rilevazione cifrata che, in caso di necessità, permettano la lettura delle impronte digitali.

In considerazione della particolare natura delle informazioni biometriche e dell'assenza di norme specifiche, l'Autorità ha valutato entro quali limiti possa considerarsi lecita, nell'ambito della realtà bancaria, l'installazione di sistemi di acquisizione criptata delle impronte digitali e quali debbano essere le imprescindibili garanzie da assicurare per il rispetto dei diritti fondamentali delle persone.

Oggi l’evoluzione tecnologica se da un lato ha reso sempre più semplici ed accessibili i meccanismi attraverso i quali la pretesa di solitudine dell’individuo tende ad essere compressa, dall’altro ha offerto forme di protezione e di prevenzione dalle intrusioni indesiderate che consentono di risolvere o quanto meno di attenuare in radice questo fenomeno. Cosicché diventa essenziale non tanto evitare che altri violino il pur diritto fondamentale di essere lasciati soli, quanto consentire che ogni individuo possa disporre di un agile diritto di controllo rispetto alle tante informazioni di carattere personale che altri possano aver assunto.

Difatti, nell'attuale era tecnologica le caratteristiche personali di un individuo possono essere tranquillamente scisse e fatte confluire in diverse banche dati, ciascuna di esse contraddistinta da una specifica finalità. Su tale presupposto può essere facilmente ricostruita la c.d. *persona elettronica* attraverso le tante tracce che lascia negli elaboratori che annotano e raccolgono informazioni sul suo conto.

Si deve ricordare innanzitutto che l’obiettivo delle nuove tecnologie è quello di migliorare la qualità della vita dei cittadini nel rispetto della sicurezza e della privacy. Qualsiasi problematica inerente i rapporti tra nuove tecnologie e privacy va sempre risolta inquadrandola nell’ambito di una considerazione globale dei benefici socio-economici che scaturiscono dall’innovazione tecnologica. Ad esempio non possono trascurarsi i grandi vantaggi rappresentati dalle banche dati presenti in Rete oltre che nello svolgimento dell’attività amministrativa, anche nel migliorare in generale la qualità della vita dei cittadini e nel promuovere le attività produttive ed economiche.

Allo stato attuale, quindi, sono evidenti, sia il timore che la semplificazione delle procedure e la dimensione globale delle reti informatiche possano tradursi in un appiattimento e svuotamento dei diritti delle persone fisiche e giuridiche, sia la consapevolezza della oggettiva utilità di tali strumenti che trascendono l'ambito nazionale sia la necessità di armonizzare quei diritti con la realizzazione di interessi pubblici e collettivi, dando attuazione, anche nel nostro ordinamento, alle applicazioni comunitarie in materia.

Con l’approvazione del decreto legislativo n. 196 del 30 giugno 2003, il quadro delle misure di protezione dei dati personali è stato profondamente modificato. I meccanismi di adeguamento previsti renderanno il Codice meno soggetto all’obsolescenza di fronte all’avanzare delle tecnologie, restando peraltro immune da tecnicismi e mantenendo invece una sufficiente generalità e indipendenza da specifiche tecnologie.

In particolare è necessario che qualsiasi trattamento di dati personali, specie se sensibili, sia rispettoso dell’art. 3 del Codice in materia di trattamento di dati personali che sancisce il principio di necessità.

Ma ciò ovviamente non è sufficiente e l’Autorità Garante con i suoi interventi ha previsto una serie di prescrizioni che devono essere attuate nello specifico settore delle nuove tecnologie con particolare riferimento alle Rfid ed ai sistemi biometrici.

Le prescrizioni

Oltre al principio di necessità va rispettato il principio di liceità (art. 11, comma 1, lett. a), del Codice). Il trattamento mediante questi nuovi sistemi è lecito solo se si fonda su uno dei presupposti che il Codice prevede, rispettivamente, per i soggetti pubblici da un lato (svolgimento di funzioni istituzionali: artt. 18-22) e, dall'altro, per soggetti privati ed enti pubblici economici (ad es., adempimento ad un obbligo di legge, o consenso libero ed espresso: artt. 23-27).

Il titolare *(art. 4, comma 1, lett. f))* può trattare dati personali esclusivamente per scopi determinati, espliciti e legittimi *(art. 11, comma 1, lett. b)*). I dati possono essere inoltre utilizzati soltanto in termini compatibili con la finalità per la quale sono stati originariamente raccolti; devono essere conservati per il tempo strettamente necessario a perseguire tale finalità, decorso il quale devono essere cancellati o resi anonimi *(art. 11, comma 1, lett. b) e e) del Codice)*.

Il titolare deve verificare il rispetto del principio di proporzionalità in tutte le diverse fasi del trattamento. I dati trattati e le modalità del loro trattamento, anche con riferimento alla tipologia delle infrastrutture di rete adoperate, non devono risultare sproporzionati rispetto agli scopi da prefissare.

Il titolare del trattamento, nel fornire agli interessati la prescritta informativa precisando anche le modalità del trattamento *(art. 13 del Codice)*, deve indicare la presenza di etichette *RFID o sistemi biometrici* e specificare che, attraverso gli stessi strumenti è possibile raccogliere dati personali senza che gli interessati si attivino al riguardo.

Il titolare del trattamento deve agevolare l'esercizio, da parte dell'interessato, dei diritti di cui all'art. 7 del Codice, semplificando le modalità e riducendo i tempi per il riscontro al richiedente *(art. 10, comma 1 del Codice)*.

In particolare, poi, per i sistemi biometrici, l’utilizzazione dei sistemi di rilevazione cifrata delle impronte digitali deve essere riferita a situazioni di rischio, valutate anche sulla base di concordanti valutazioni da parte dei locali organi competenti per l’ordine e la sicurezza pubblica.

La rilevazione delle impronte non può dar luogo ad alcuna "schedatura" da parte degli istituti di credito che, quindi, non potranno costituire alcuna banca dati con le informazioni raccolte.

Le informazioni relative alle impronte devono essere rigorosamente protette da sistemi di cifratura automatica sin dal momento della loro acquisizione. Non saranno quindi immediatamente riconducibili a persone e l'eventuale associazione alle immagini, rilevate con telecamere, potrà avvenire solo dopo la decrittazione.

Soltanto l’autorità giudiziaria o di polizia, e solo nell’ambito di indagini connesse alla commissione di reati, potrà decifrare ed avere accesso alle informazioni.

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