FABINFORMA
NOTIZIARIO A CURA DEL COORDINAMENTO NAZIONALE
BANCHE DI CREDITO COOPERATIVO

GARANTE DELLA PRIVACY

PuntoSicuro di giovedì 11 maggio 2006

BIOMETRIA E PRIVACY

Dal Garante un decalogo che sintetizza le regole sull'utilizzo dei dati biometrici. Indicazioni per progettisti, costruttori di sistemi e utenti.

Sintetizza i provvedimenti emanati dal Garante della privacy in tema di utilizzo dei dati biometrici il decalogo presentato da Giuseppe Fortunato, componente dell'Autorità, in occasione di Forum PA.

Il documento è una guida operativa destinata non solo a chi progetta e costruisce sistemi per la rilevazione di dati corporei, ma anche a ogni cittadino, affinché possa riconoscere, e segnalare, eventuali abusi.

Illustrando il vademecum, che non esonera ovviamente dall'osservanza puntuale dei provvedimenti del Garante in materia, il Garante ha affermato: "Ben vengano le innovazioni tecnologiche; la ricerca scientifica in materia sta producendo di giorno in giorno nuove possibilità applicative attraverso la raccolta e l'uso dei dati biometrici. L'impegno di tutti è che la ricerca di nuove tecniche vada sempre di pari passo con la dignità umana. […] Il corpo non è una password e va rispettato inderogabilmente."

Questi i dieci punti che devono essere rispettati nell'utilizzo e nella progettazione di sistemi biometrici:

1. Affidabilità del sistema di rilevazione dei dati corporei, indicando il livello della sua accuratezza. La rigorosità dei controlli (preventivi e indubitabili negli esiti) deve tener conto anche di valutazioni di comitati tecnici indipendenti.
2. Informativa chiara, lasciando comunque la libertà di aderire o meno al sistema, salvo stringenti ragioni, indicando nella stessa informativa espressamente le tecniche alternative all'utilizzo dei dati corporei.
3. Liceità verificabile indubitabilmente sotto i profili di necessità, proporzionalità, finalità, correttezza, adeguatezza e qualità dei dati, previa acclarata dimostrazione dell'inefficacia di pratiche alternative che abbiano meno rischi di profilabili abusi. In particolare, qualora l'uso dei dati corporei sia permesso, deve essere comunque il più possibile circoscritto (ad esempio impronta di un dito invece di più dita).
4. Deroga motivata con uso controllato in speciali casistiche e non uso generalizzato o incontrollato o indifferenziato. Tale deroga motivata va periodicamente riesaminata, valutando la persistente sussistenza dei fattori che l'hanno determinata, anche alla luce del progresso scientifico.
5. Delimitata memorizzazione su circoscritti supporti correlati sempre disponibili per l'interessato e non centralizzazione sotto qualsiasi forma ed in particolare divieto assoluto di archivi centralizzati, anche se con dati cifrati. In particolare occorre attivare una funzione permanente di ricerca di soluzioni che evitino accumulazioni o unificazioni di dati.
6. Temporanea conservazione in ordine cronologico per il necessario periodo limitato (e, come nel caso di associazione di dati biometrici con videoregistrazioni, per non oltre una settimana). Sono vietati, in particolare, le cosiddette copie di sicurezza che prolungano surrettiziamente i tempi di conservazione.
7. Scrupolose misure di sicurezza con sistemi inequivoci e senza rischio, promuovendo, come obbligatoriamente ed inderogabilmente infatti nel caso di uso congiunto di dati biometrici e di videosorveglianza in banca, l'interposizione di un "vigilatore dei dati" indipendente, individuato nel titolare di una funzione in posizione di indipendenza o da un soggetto indipendente (anche proceduralmente non essendo designato dall'organo ammninistrativo bensì dall'organo indipendente). In particolare nei casi prescritti va evitata anche la sola teorica possibilità di decifrare le informazioni acquisite senza l'intervento di tale vigilatore.
8. Piena ed immediata conoscibilità dei dati biometrici da parte dell'interessato e limitazioni stringenti (sino al completo divieto nel caso di uso incrociato di dati biometrici e videosorveglianza) per datore di lavoro, suoi dipendenti e collaboratori. Per le operazioni inerenti alla conoscenza, va promossa, ove necessaria, la cooperazione di un vigilatore indipendente (obbligatorio e inderogabile nel caso di uso incrociato di dati biometrici e videosorveglianza).
9. Rispetto rigoroso degli obblighi di verifica preliminare del Garante (art. 17 Codice Privacy) e di notifica al Garante (art. 37 Codice Privacy).
10. Disattivazione automatica, immediata e certa di funzioni di smart card o altre analoghe nel caso di smarrimento o di furto.