Temi: Biometria
Categoria professionale: Direzione dei sistemi di sicurezza
Tipologia di dati: Biometrici

Come mettere in opera il sistema biometrico?

Un'impresa decide di rafforzare il proprio sistema di sicurezza introducendo un controllo biometrico per l'accesso agli edifici dei dipendenti.
La direzione incarica il servizio di sicurezza informatico di sviluppare un sistema d'identificazione biometrico.
L'uso della biometria può presentare dei rischi importanti, legati soprattutto alle possibilità di monitorare degli individui e d'interconnessione delle informazioni e delle banche dati.
La direzione dei sistemi d'informazione (DSI) propone due soluzioni alla direzione generale: o una tecnologia basata sullo stoccaggio di sagome su un supporto di cui la persona interessata abbia un uso esclusivo (scheda magnetica, cellulare, computer portatile, ecc.), oppure ricorrere a un elemento biometrico che non lasci traccia, come il contorno della mano.
Per evitare discriminazioni, è necessario prevedere delle alternative per le persone che non sono in grado di utilizzare un sistema biometrico. L'identificazione dei dati biometrici deve farsi unicamente confrontando un campione prelevato dalla persona interessata. I dati biometrici originali devono essere distrutti una volta conclusa la procedura di registrazione.

Raccomandazioni
Lo scopo prefigurato deve essere chiaro e deve essere scelta la misura più adeguata, necessaria e meno invasiva per raggiungerlo. Questa misura deve fare oggetto di una comunicazione appropriata. Il datore di lavoro dovrebbe informare e consultare i suoi dipendenti o i loro rappresentanti e se possibile ottenere il loro consenso prima d'introdurre dei sistemi automatizzati per la raccolta e il trattamento dei dati personali.

Prinicipi di base
LIPAD 38 et 42 ; LPD 4; 12 e 13 ; LL 6 ; OLL3 26 ; CO 328 e 328*b*

Protezione della personalità, protezione dei lavoratori, principi di liceità (legalità), di buona fede e di proporzionalità: la misura deve essere adeguata, necessaria e la meno invasiva possibile.

Esempio concreto
La banca privata Pictet & Cie di Ginevra usa il riconoscimento facciale in 3D come misura di sicurezza per l'accesso ai suoi edifici dal 2006. Com'è riuscita a sormontare i timori dei suoi 2000 collaboratori? Grazie alla comunicazione. Questa tecnologia non permette di monitorare lo stato di salute di un individuo e di violare la sua sfera privata. « I dipendenti temono a volte che la scannerizzazione del loro viso sia pericoloso per la salute, ma non è assolutamente così poiché l'apparecchio non fa che filmarli », nota Jean-Pierre Therre, responsabile della sicurezza della banca privata. La banca dati non contiene foto degli impiegati, ma unicamente l'analisi delle scannerizzazioni del loro cranio secondo 40.000 punti di riferimento: http://www.1234economy.com/biometrie-et-reconnaissance-faciale-en-3d-comment-la-banque-privee-genevoise-pictet-a-gere-les-resistances / .