Temi: Biometria
Categoria professionale: Impiegato
Tipologia di dati: Biometrici

Hanno il diritto di esigere la raccolta dei miei dati biometrici?

Un impiegato utilizza una chiave magnetica per accedere al suo luogo di lavoro. La direzione decide di cambiare il controllo magnetico degli accessi con un controllo biometrico (impronte retiniche o geometria della mano e impronte digitali). Annuncia il cambiamento al personale.
Per informarsi, l'impiegato chiama un sindacato che gli spiega che è « completamente illegale », che il personale dovrebbe « rifiutare di partecipare » e che un licenziamento per questo motivo « sarebbe altamente abusivo ». L'impiegato informa il suo superiore gerarchico che non ha l'intenzione di sottomettersi alla raccolta delle impronte.
Informata dall'intenzione dell'impiegato, la direzione gli fa capire che considererebbe questa mancanza di collaborazione come una violazione non ammissibile del contratto di lavoro.
Preoccupato, il superiore gerarchico si appella al consigliere (o responsabile) della protezione dei dati e organizza una seduta con un rappresentante della direzione per valutare la situazione.
Al termine della seduta, viene ammesso che la raccolta dei dati progettata non è proporzionata allo scopo perseguito e che sarebbe dunque necessario ottenere il consenso di ciascun impiegato. La direzione aggiorna il suo progetto e promette di studiare una soluzione meno invasiva.
I dati raccolti per permettere un controllo biometrico possono essere usati a dei fini estranei allo scopo annunciato. L'impiegato è soddisfatto che i suoi timori siano stati ascoltati.

Raccomandazioni
I dati biometrici comprendono generalmente dei dati sensibili (in particolare sulla salute). Quand'è così, una base legale formale è necessaria e le persone interessate devono essere chiaramente informate e dare il loro consenso al trattamento di questi dati. Lo scopo prefigurato deve essere chiaro e deve essere scelta la misura la più adeguata e meno invasiva per raggiungerlo. Questa misura deve fare oggetto di una comunicazione appropriata. Il datore di lavoro deve inoltre consultare gli impiegati o i loro rappresentanti e, in assenza di una base legale formale, ottenere il loro consenso libero e informato prima d'introdurre dei sistemi automatizzati per il trattamento dei dati personali.

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

Protezione della personalità, protezione dei lavoratori, principio della proporzionalità: la misura deve essere necessaria e il meno invasiva possibile.

Esempio concreto
La banca privata Pictet & Cie di Ginevra usa il riconoscimento facciale in 3D come misura di sicurezza d'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 /