

**Temi:** Biometria

**Categoria professionale:** Direzione delle risorse umane (DRU)

**Tipologia di dati:** Biometrici

## Il controllo biometrico d'accesso ai locali rispetta l'integrità personale dei dipendenti?

La direzione generale ha deciso di rimpiazzare il controllo magnetico degli accessi con un controllo biometrico (impronte retiniche o geometria della mano e impronte digitali). Annuncia il cambiamento al personale. La commissione del personale si riunisce.

Al termine di una discussione animata, la commissione del personale decide di ostacolare la realizzazione del progetto della direzione.

La direzione delle risorse umane (DRU) è presa tra due fuochi. Da un lato, quest'ultima, convinta dei vantaggi del dispositivo, non vuole cambiare idea, dall'altro la commissione del personale sostiene che l'impiego di un tale dispositivo costituirebbe una violazione dell'integrità personale dei dipendenti. La DRU organizza una seduta con la direzione dei servizi d'informazione (DSI), la direzione generale e il consigliere (o responsabile) della protezione dei dati per valutare le possibili soluzioni.

Alla fine della seduta, viene riconosciuto il fatto che la raccolta dei dati progettata non è proporzionata allo scopo prefigurato e che sarebbe dunque necessario ottenere il consenso di ciascun dipendente. Visto il costo e le complicazioni che sarebbero generati con la presenza di due dispositivi paralleli (magnetico e biometrico), la direzione generale rimanda la realizzazione del suo progetto e chiede alla DSI di studiare una soluzione meno invasiva.

I dati raccolti per il controllo biometrico possono essere impiegati a fini estranei allo scopo annunciato. La DRU è soddisfatta d'aver potuto favorire la ricerca di una soluzione rispettosa dell'integrità personale dei dipendenti.

### Raccomandazioni

I dati biometrici comprendono generalmente dei dati sensibili (in particolare quelli sulla salute). Se questi dati sensibili vengono rilevati è necessaria una base legale formale e le persone coinvolte devono essere chiaramente informate e consentire il trattamento di questi dati. Lo scopo prefigurato deve essere chiaro, e deve essere scelta la misura necessaria più appropriata e meno invasiva per raggiungerlo. Questa misura deve fare oggetto di una comunicazione adeguata. Il datore di lavoro deve inoltre consultare i suoi dipendenti 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.

### Principi 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 di 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 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 né 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/>