

Il datore di lavoro può chiedere le impronte al dipendente?



Per il Garante privacy l'uso dei dati biometrici per il rilevamento delle presenze non può avvenire senza una base normativa: così il trattamento è illecito.

La tecnologia sta penetrando in tutti gli aspetti della vita quotidiana, compresa la timbratura del cartellino sul luogo di lavoro. Alcuni datori si stanno attrezzando con metodi di rilevamento biometrico, che identificano ciascun dipendente in base alle sue caratteristiche fisiche. Se vuoi entrare in ufficio o in azienda devi passare attraverso il rilevatore biometrico e fornire le tue impronte digitali.

Ma questo metodo è legittimo in base alla normativa sulla privacy, che garantisce la riservatezza dei dati personali? **Il datore di lavoro può chiedere le impronte al dipendente?** Secondo l'Autorità Garante no, almeno fino a quando non sarà introdotta un'adeguata base normativa che stabilisca i metodi da utilizzare e le garanzie degli interessati. Così un'azienda sanitaria siciliana, che aveva applicato questo rilevamento delle presenze in base alle impronte digitali dei suoi oltre 2mila dipendenti, è stata sanzionata per illecito trattamento dei dati biometrici.

Il trattamento di dati biometrici

Il **trattamento di dati personali** di tipo biometrico riguarda tutte le operazioni che consentono di identificare un soggetto: tra le caratteristiche corporee più frequentemente utilizzate ci sono la voce, il riconoscimento facciale, l'occhio (iride o retina) e le impronte digitali.

Ai sensi della normativa sulla privacy [1], i **dati biometrici** sono definiti come «dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i **dati dattiloscopici**». Per la loro univocità, essi sono inseriti nella categoria dei **dati sensibili** [2] che, come vedremo ora, è tutelata con maggiori garanzie rispetto ai dati "comuni".

Il riconoscimento mediante le impronte digitali

I dati biometrici vengono utilizzati frequentemente nella pratica e, spesso, il **riconoscimento** già avviene mediante le **impronte digitali**. Ad esempio, per sbloccare gli smartphone di ultima generazione si usa il dito dell'utilizzatore: questo è un sistema per identificare in modo pressoché certo il proprietario dell'apparecchio, con l'ulteriore vantaggio che il riconoscimento avviene in modo univoco e molto più sicuro rispetto ai consueti codici e password che potrebbero essere carpiri da altri.

La rilevazione delle presenze sul lavoro mediante impronte digitali

Questo metodo, per la sua sicurezza e per le funzionalità che offre, si è esteso molto al di là dell'uso dei dispositivi personali di connettività ad Internet ed è arrivato a riguardare anche la **rilevazione delle presenze sul lavoro** dei dipendenti.

Il dato biometrico rilevato attraverso la **lettura dell'impronta digitale** viene codificato e trasformato in un **codice numerico**, che viene archiviato dal sistema

informatico del datore di lavoro e può essere inserito anche nel **badge dei dipendenti** stessi, in maniera da facilitare il loro riconoscimento ad ogni accesso sul luogo di lavoro.

Alcuni esperti di privacy al riguardo hanno parlato di una “**schedatura**” dei dipendenti attraverso le loro specifiche **caratteristiche dattiloscopiche** individuali e immutabili: le impronte digitali andrebbero, invece, gestite con la massima cura, predeterminando i modi di acquisizione e di conservazione e adottando tutte le cautele necessarie ad impedirne la divulgazione non autorizzata e qualsiasi altro utilizzo illecito.

Uso delle impronte digitali da parte del datore di lavoro e normativa privacy

Alcuni **datori di lavoro** hanno sostenuto che questa sequenza numerica ricavata dalle impronte digitali non costituisca un trattamento di dati personali e che il lavoratore continuava ad essere identificato sempre attraverso il badge, ma la Corte di Cassazione già in passato **[3]** ha respinto questa tesi ed ha affermato che la suddetta trasformazione delle impronte in codici è irrilevante in quanto attraverso l’algoritmo si può sempre **risalire al lavoratore** al quale appartiene il dato.

Perciò, in tali casi, deve essere rispettata la **normativa sulla privacy**, che prevede, innanzitutto, la notifica del trattamento da parte dell’azienda al Garante per la protezione dei dati personali.

Quando l’azienda è sanzionata per trattamento illecito di dati biometrici personali

Ora, è lo stesso **Garante privacy** ad intervenire direttamente nella questione: con un apposito provvedimento **[4]** ha sanzionato un’azienda sanitaria provinciale per l’utilizzo di un **sistema di rilevazione delle presenze** basato sul trattamento di dati biometrici dei dipendenti.

Nel caso esaminato, è emerso che la base normativa attuata da parte della

struttura sanitaria era carente ed inoltre, pur avendo l'azienda informato il personale e i sindacati della scelta organizzativa compiuta, non aveva fornito tutte le **informazioni sul trattamento**, come richiesto dal Regolamento europeo in materia di privacy.

L'illegittimità del rilevamento delle impronte digitali dei lavoratori

L'Authority ha affermato che «per installare questo tipo di sistemi è necessaria una **base normativa** che sia proporzionata all'obiettivo perseguito e che fissi misure appropriate e specifiche per tutelare i diritti degli interessati». In particolare, le norme devono «stabilire **garanzie** per circoscrivere gli ambiti di applicazione e regolare le principali modalità del trattamento».

Ma nel caso esaminato non c'era alcun regolamento emanato per disciplinare tali attività. Ciò nonostante, «l'Azienda verificava l'**identità del dipendente** mediante il confronto tra il modello biometrico di riferimento, memorizzato all'interno del badge, e l'**impronta digitale** presentata all'atto del rilevamento della presenza e trasmetteva il numero di matricola del dipendente, la data e l'ora della timbratura, al sistema di gestione delle presenze».

In questo modo, il **trattamento dei dati personali biometrici** dei dipendenti era duplice: avveniva - come ha osservato il Garante - «sia all'atto dell'emissione del badge, sia all'atto della verifica dell'impronta in occasione di ogni "**timbratura**" di ciascun dipendente» e tutto ciò «in assenza di una idonea base giuridica».

Il consenso dei dipendenti all'utilizzo delle impronte digitali

Il **consenso** manifestato dai **dipendenti** può valere a rendere lecita tale condotta del datore di lavoro? Per l'Autorità Garante no: «non può essere considerato valido, nel contesto lavorativo, a maggior ragione pubblico, per effetto dello squilibrio del rapporto tra dipendente e datore di lavoro».

Per questi motivi, il Garante ha dichiarato **illecito** il **trattamento dei dati biometrici** ed ha applicato all'Asp 30.000 euro di sanzione. Ha inoltre disposto la

cancellazione dei modelli biometrici memorizzati all'interno dei badge e chiesto all'Asp di far conoscere le iniziative che intende intraprendere per far cessare il trattamento dei dati biometrici dei dipendenti.

È lecito rilevare le presenze dei dipendenti con le impronte digitali?

Visto l'orientamento espresso dal Garante, allo stato attuale, non è possibile **rilevare le presenze dei dipendenti** attraverso le **impronte digitali**, neppure quando esse vengono codificate ed inserite nel badge del lavoratore. Si potrà adottare questo metodo solo quando sarà introdotta l'apposita normativa auspicata dal Garante, necessaria per regolamentare il trattamento dei dati biometrici e tutelare adeguatamente **i diritti dei lavoratori** interessati.