Digeat N.2 - 19 Giugno 2024

Il trattamento dei dati biometrici in ambito lavorativo: digitale, ma non troppo

Di Anna Perut

Abstract

Il Garante per la protezione dei dati personali è tornato recentemente a pronunciarsi sul trattamento dei dati biometrici in ambito lavorativo, ribadendo che al momento il nostro ordinamento non consente ai datori di lavoro di ricorrere a sistemi di rilevamento biometrici per la registrazione delle presenze dei dipendenti. Viviamo in un contesto in cui i sistemi di autenticazione biometrica sono sempre più diffusi, accediamo ai nostri smartphone con l'impronta digitale o il riconoscimento facciale, eppure non è possibile registrare le presenze del personale con queste metodologie. Per quale motivo? Esaminando il contesto normativo e i principi generali in materia di protezione dati, anche alla luce delle indicazioni del nostro Garante, emerge come, ad oggi, i tempi non siano ancora maturi per dare una lettura diversa rispetto all'orientamento ormai consolidato, con buona pace dei datori di lavoro più inclini alle innovazioni tecnologiche.

Indice

Le aziende che avessero l'intenzione di adottare sistemi di rilevazione delle presenze dei propri dipendenti mediante sistemi biometrici dovranno, almeno per il momento, abbandonare l'idea e propendere per i metodi più tradizionali.

Il Garante per la protezione dei dati personali è tornato infatti recentemente sull'argomento pronunciando una serie di **provvedimenti sanzionatori** nei confronti di alcune aziende che avevano introdotto dei sistemi di rilevamento delle presenze sui luoghi di lavoro mediante riconoscimento facciale (si veda la Newsletter del Garante del 28.03.2024).

> La posizione del Garante potrà sembrare di difficile comprensione, dopotutto ogni giorno accediamo ai nostri dispositivi mediante sistemi biometrici. Perché possiamo sbloccare lo smartphone inquadrando il nostro volto, ma non possiamo "timbrare il cartellino" con lo stesso sistema? In questo modo probabilmente la gestione degli accessi sarebbe più rapida, si eviterebbero gli inghippi derivanti dalle dimenticanze delle timbrature, oltre ad esserci indubbi vantaggi in termini di lotta all'assenteismo.

La spiegazione ci viene data dall'Autorità Garante, la quale, con queste ordinanze (molto simili nei contenuti, stante l'analogia dei trattamenti oggetto di accertamento), ripercorre **le caratteristiche dei**

trattamenti dei dati biometrici nel contesto lavorativo, **le basi giuridiche e i principi generali**, facendo un excursus ragionato che permette di inquadrare l'argomento in modo chiaro e approfondito.

Cosa sono i dati biometrici?

I dati biometrici sono definiti come "*i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*" (art. 4, par. 1 n. 14 Regolamento UE 679/16 – GDPR). Per intenderci, il riconoscimento facciale piuttosto che il rilevamento delle impronte digitali o la scansione dell'iride comportano tutti il trattamento di dati biometrici.

Tali dati, stante la loro capacità di identificare l'individuo a cui appartengono in modo diretto, univoco, e tendenzialmente stabile nel tempo, sono dati **considerati ad alta criticità che rientrano nella categoria dei dati particolari, il cui trattamento è di regola vietato**, salvo che ricorra una delle condizioni di liceità indicate dall'art. 9, par. 2, GDPR.

> Il trattamento di dati biometrici prevede sostanzialmente due fasi: la prima, che consiste nel rilevamento (c.d. "enrolment") tramite specifici dispositivi delle caratteristiche biometriche dell'interessato (es. impronta, volto), chiamate "campione biometrico", dal quale si estrae il "modello biometrico", ovvero la rappresentazione digitale della caratteristica biometrica, che viene conservata per il successivo confronto. La seconda fase è quella del riconoscimento biometrico, che consiste nel confronto tra il modello biometrico e il modello o i modelli precedentemente acquisiti.

I sistemi possono essere utilizzati sia per l'**identificazione biometrica**, ovvero il processo in cui il sistema confronta il modello rilevato con tutti i modelli disponibili nel database per individuare l'identità del soggetto (c.d. confronto uno-a-molti), sia per la **verifica biometrica**, cioè il processo in cui il soggetto dichiara la sua identità e il sistema effettua un confronto tra il modello biometrico rilevato e quello memorizzato e corrispondente all'identità dichiarata (c.d. confronto uno-a-uno).

In questo caso il sistema confronta un modello o un campione biometrico precedentemente registrato e conservato o in una banca dati centralizzata, oppure in modo decentralizzato, ad esempio sul dispositivo di rilevazione o su dispositivi custoditi dall'interessato, con il modello biometrico ricavato dalle caratteristiche dell'individuo al momento della richiesta di riconoscimento, al fine di verificare che si tratti della medesima persona.

La base giuridica nel contesto lavorativo

Nell'ambito lavorativo, il trattamento di dati particolari, tra i quali rientrano, come abbiamo visto, i dati biometrici, è lecito solo se "*necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato*" (si veda art. 9, par. 2 lettera b) GDPR).

> Se è pacifico che il trattamento di dati personali per la rilevazione delle presenze del personale possa rientrare nei trattamenti ammessi in quanto necessari nel contesto lavorativo, è altrettanto vero il trattamento, per essere lecito, deve essere anche autorizzato da una legge interna o europea, in presenza di garanzie adeguate, e al momento l'attuale quadro normativo non prevede il trattamento di dati biometrici per queste finalità.

In questo scenario, il **ricorso al consenso dell'interessato come possibile base giuridica** per legittimare il trattamento dei dati biometrici **non è una strada percorribile**.

Nel contesto lavorativo, infatti, il consenso di regola non costituisce un valido presupposto di liceità dei trattamenti in considerazione della **asimmetria tra la posizione del datore di lavoro e quella del dipendente**, il quale difficilmente potrà prestare il proprio consenso libero ed incondizionato ad un determinato trattamento senza sentire pressioni da parte del datore di lavoro (si vedano sul punto le Linee Guida EDPB 5/2020 sul consenso ai sensi del regolamento (UE) 2016/67, adottate il 4/05/2020; WP 29 Opinion 2/2017 on data processing at work – WP 249). Sul punto, significativo è il fatto che il Garante non abbia ritenuto conforme neanche la soluzione di prevedere un sistema di rilevamento presenze tradizionale in alternativa a quello biometrico, da utilizzare quindi su base volontaria (si veda il Provvedimento del Garante del 10 novembre 2022 n. 369; Provvedimento del Garante del 22 febbraio 2024 n. 105).

Non è percorribile neanche la strada del legittimo interesse dell'azienda a combattere l'assenteismo sul posto di lavoro, ai sensi dell'art. 6, par. 1 lettera f) GDPR, trattandosi di una base giuridica non applicabile ai dati particolari. **I casi in cui l'Autorità ha legittimato il ricorso alla biometria ritenendo il sistema proporzionato rispetto alla finalità di scongiurare l'uso distorto dei sistemi di rilevamento presenze di uso comune sono piuttosto limitati** e relativi a contesti peculiari nei quali i ripetuti episodi di violazione dei doveri d'ufficio da parte dei dipendenti, la particolare conformazione strutturale dell'azienda e l'esigenza di garantire la continuità dei servizi a favore della collettività hanno determinato il Garante ad autorizzare il predetto trattamento (si veda il Provvedimento del 15 settembre 2016 n. 357).

> Al di fuori, quindi, di queste limitate ipotesi, il trattamento in questione appare privo di una valida base giuridica ai sensi dell'art. 9 GDPR e non appare conforme ai principi di liceità, correttezza, minimizzazione e proporzionalità, posto che il datore di lavoro potrebbe perseguire le medesime finalità (la registrazione delle presenze) con metodologie meno invasive per i diritti degli interessati (es. controllo mediante badge o fogli presenze).

Queste tematiche sono state oggetto di analisi anche da parte dell'**Autorità Garante Spagnola (AEPD)** nelle recenti Linee guida per il trattamento dei dati biometrici durante il controllo delle presenze e l'accesso ai locali del novembre 2023, ove giunge a conclusioni in linea con la nostra Autorità. In questo documento il Garante spagnolo fornisce interessanti spunti di riflessione, evidenziando come, anche ammettendo un sistema biometrico su base volontaria come alternativo rispetto ai sistemi tradizionali, ai quali il dipendente potrebbe aderire in qualsiasi momento, questo implicherebbe che il trattamento di dati biometrici non sarebbe necessario per la finalità concreta, diventando automaticamente non conforme ai principi generali.

Le possibili eccezioni: casi di liceità dei trattamenti biometrici

I trattamenti di dati biometrici nell'ambito lavorativo non sono da considerarsi sempre illeciti. Il Garante, infatti, nel Provvedimento generale prescrittivo in tema di biometria del 12.11.2014, da ritenersi ancora attuale, aveva individuato alcune tipologie di trattamenti che, per le specifiche finalità perseguite, la tipologia di dati trattati e le misure di sicurezza concretamente applicabili, presentavano un rischio ridotto e pertanto erano **considerati conformi alla normativa e non soggetti alla richiesta di verifica preliminare** ai sensi dell'art. 17 del previgente Codice Privacy.

Tra i possibili trattamenti biometrici che possono configurarsi negli ambiti lavorativi rientrano i controlli di accesso fisico ad aree "sensibili" dei soggetti addetti e l'utilizzo di apparati e macchinari pericolosi. In questi casi, il Garante ammette l'utilizzo ad esempio delle impronte digitali al fine di **consentire l'utilizzo di determinati macchinari particolarmente pericolosi ai soli soggetti addetti** e **qualificati** oppure per **accedere ad aree ritenute sensibili nelle quali è necessario innalzare il**

livello di sicurezza, quali ad esempio locali ove sono conservati beni di particolare valore o informazioni o documenti di particolare segretezza, **aree preposte allo svolgimento di processi produttivi pericolosi** che richiedono un accesso selezionato. In questi casi l'Autorità afferma che, qualora il trattamento avvenga nel rispetto delle indicazioni impartite, le esigenze specifiche di sicurezza del Titolare del trattamento permettono di effettuare il trattamento senza richiedere il consenso dei dipendenti. **Si tratta quindi di contesti specifici molto diversi dalle rilevazioni delle presenze dei dipendenti.**

Nel Provvedimento citato e nelle relative Linee Guida di cui all'Allegato A il Garante elenca una serie di prescrizioni e di misure di sicurezza che devono necessariamente essere rispettate e che costituiscono sicuramente una base di partenza da interpretarsi alla luce dell'art. 32 GDPR.

> In questi casi il Titolare, per svolgere un trattamento a norma, dovrà applicare robuste misure di sicurezza sia nella fase di *enrolment,* sia nella successiva fase di riconoscimento, mediante tecniche crittografiche. Dovrà essere effettuata una accurata valutazione sulle modalità e luoghi di conservazione dei dati biometrici, privilegiando, ove tecnicamente possibile, la conservazione dei soli modelli biometrici su dispositivi nella sola disponibilità dell'utente, con cancellazione di ogni altra copia di dati, evitando l'archiviazione centralizzata su banche dati. Particolare attenzione dovrà essere prestata alle tempistiche di conservazione dei dati, agli obblighi informativi verso gli interessati e alla corretta definizione dei ruoli dei possibili soggetti coinvolti nel trattamento, quali amministratori di sistema e responsabili del trattamento.

La valutazione d'impatto ai sensi dell'art. 35 GDPR è d'obbligo, trattandosi di dati biometrici di dipendenti (considerati soggetti vulnerabili) trattati mediante nuove tecnologie.

In conclusione

Il panorama di riferimento è dunque questo. L'azienda virtuosa, che non può ignorare i precedenti consolidati del Garante, deve, almeno per il momento, **fare un passo indietro e astenersi dall'introdurre sistemi biometrici di rilevamento delle presenze**, mantenendo un approccio che a prima vista potrebbe essere interpretato come una chiusura rispetto all'evoluzione tecnologica globale ma che risulta invece conforme ai principi normativi e volto alla effettiva protezione dei diritti e delle libertà degli interessati.