DPO st
YOUR DATA PROTECTION JOURNAL

10 aprile 2024 Newsletter 01

Dati biometrici e riconoscimento facciale: il no del Garante per il controllo delle presenze dei dipendenti

Profili *data protection* e di *compliance* al GDPR

> Al fine del trattamento dei **dati biometrici dei dipendenti e/o collaboratori**, la prestazione del **consenso** da parte di questi ultimi **non può costituire, di regola, un valido presupposto di liceità** per il trattamento dei dati personali in ambito lavorativo, indipendentemente dalla natura pubblica o privata del datore di lavoro, alla luce della asimmetria tra le rispettive parti del rapporto di lavoro e la conseguente, eventuale, necessità di accertare di volta in volta e in concreto l'effettiva libertà della manifestazione di volontà del dipendente.
>
> Ciò, tenendo in considerazione anche l'esistenza di strumenti **meno invasivi** per controllare la presenza dei propri dipendenti e/o collaboratori sul luogo di lavoro, per cui il trattamento del **dato biometrico** nel contesto dell'ordinaria gestione del rapporto di lavoro **non** appare **conforme** ai **principi di minimizzazione e proporzionalità** del trattamento.

Premessa

Il Garante per la protezione dei dati personali ("**Garante**" o "**Autorità**") il 22 febbraio 2024 ha sanzionato cinque società per aver trattato i **dati biometrici di un numero significativo di lavoratori** attraverso l'impiego di **sistemi di riconoscimento facciale** per **controllare le presenze sul posto di lavoro**.

In particolare, l'Autorità – intervenuta a seguito dei reclami di diversi dipendenti delle varie società – ha accertato che tre aziende avevano condiviso per più di un anno lo stesso **sistema di rilevazione biometrica**, oltretutto senza aver adottato **misure tecniche e di sicurezza adeguate**. Inoltre, il medesimo "sistema", ritenuto illecito dall'Autorità, era utilizzato presso altre nove sedi dove operava una delle società sanzionate. Le aziende, infine, non avevano fornito una **informativa *privacy* chiara e dettagliata ai lavoratori,** né avevano effettuato la **valutazione d'impatto** sul trattamento.

I provvedimenti in questione ("**Provvedimenti**")[1], si inseriscono nel contesto di un orientamento nazionale ed europeo oramai consolidato, sul tema dell'utilizzo dei **sistemi di riconoscimento facciale** e, conseguentemente, dei **dati biometrici**, ed in particolare, sui rischi per i diritti e le libertà degli interessati connessi all'uso di tali tecnologie[2].

---

[1] Provvedimento del 22 febbraio 2024 n. 9995680, Provvedimento del 22 febbraio 2024 n. 9995701, Provvedimento del 22 febbraio 2024 n. 9995741, Provvedimento del 22 febbraio 2024 n. 9995762, Provvedimento del 22 febbraio 2024 n. 9995785.

[2] Sul punto si vedano le Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate il 29 gennaio 2020 (punti 4 e 73), Provvedimento del 14 gennaio 2021 n. 9542071, Provvedimento del 10 novembre 2022 n. 9832838, Provvedimento del 10 febbraio 2022 n. 9751362,

Un chiarimento tecnico

Preliminarmente, occorre precisare che per riconoscimento facciale si intende l'elaborazione automatica di immagini digitali contenenti volti di individui per l'identificazione o la verifica di quest'ultimi attraverso l'impiego e il confronto di modelli facciali[3]. Tale tecnica è basata sulla raccolta di dati biometrici, ossia il dato personale ottenuto da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consente o conferma l'identificazione univoca[4].

Lo stesso Garante si è più volte espresso sulle tecniche di trattamento biometrico[5], delineando le due fasi principali che lo caratterizzano:

- Fase 1: una sequenza di fasi di elaborazione a partire dal rilevamento di una determinata caratteristica biometrica, biologica o comportamentale, di un individuo, al fine di creare un campione biometrico;
- Fase 2: il c.d. *biometric enrolment*, finalizzato ad acquisire la caratteristica biometrica per consentire l'accreditamento nel sistema biometrico e il legame con il soggetto che si sottopone all'*enrolment*, nonché la qualità del campione biometrico risultante. Dai campioni biometrici è poi possibile estrarre tratti distintivi (per esempio, misurazioni del volto da un'immagine) e conservarli per sottoporli a un successivo utilizzo al posto degli stessi campioni per le successive operazioni di confronto propedeutiche al riconoscimento biometrico.

Il trattamento dei dati biometrici – come osservato dalla stessa Autorità – è riferibile tanto alla **fase di registrazione** (e quindi di *enrolment*), quanto alla **fase di effettivo *matching* e conseguente riconoscimento biometrico**, all'atto della rilevazione delle presenze.

Normativa di riferimento

Il trattamento di dati biometrici, generalmente vietato ai sensi dell'art. 9 par. 1 del Regolamento (UE) 2016/619 ("**GDPR**"), è consentito in ambito lavorativo solamente qualora il trattamento risulti necessario (i) per **assolvere gli obblighi ed esercitare i diritti specifici del titolare** o dell'**interessato** in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, (ii) 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, (iii) in presenza di **garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato**.

A tal proposito il Garante ha ribadito come, in relazione ai trattamenti di dati particolari effettuati nell'ambito del rapporto di lavoro, la **prestazione del consenso del dipendente non costituisce**, di regola, **un valido presupposto di liceità** per il trattamento dei dati personali in ambito lavorativo, indipendentemente dalla natura pubblica o privata del datore di lavoro, ciò alla luce della asimmetria tra le rispettive parti del rapporto di lavoro e la conseguente, eventuale, necessità di accertare di volta in volta e in concreto l'effettiva libertà della manifestazione di volontà del dipendente[6].

In sintesi, prima di effettuare il trattamento dei dati biometrici dei lavoratori, il datore di lavoro dovrebbe verificare in *primis* la sussistenza di un **idoneo presupposto di liceità**, rispettando le condizioni per il **lecito impiego di strumenti tecnologici nel contesto lavorativo** e **valutando i rischi per i diritti e**

adottato, seppure in un diverso contesto, in materia di riconoscimento facciale, Decreto Legge 10/5/2023, n. 51, conv. in legge 3/7/2023, n. 87, che ha prorogato al 31 dicembre 2025 la sospensione dell'installazione e utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati; European Data Protection Board, Guidelines 05/2022 *on the use of facial recognition technology in the area of law enforcement*, v. 2.0., adottate il 26 aprile 2023.

[3] Committee of Convention 108, Guidelines on facial recognition del 28 gennaio 2021.

[4] Art. 4 par. 1 Regolamento (UE) 2016/679.

[5] All. A. al Provv. 513 del 12 novembre 2014 - Linee-guida biometria.

[6] V., tra gli altri, provv. 10/11/2022, n. 369, doc. web n. 9832838.

le libertà fondamentali dei lavoratori connessi all'impiego di tali sistemi, tenendo in considerazione anche il dettato dell'art. 2- *septies* co. 7 del D. Lgs 196/2003 e ss.mm.ii. (c.d. **Codice Privacy**), secondo cui il trattamento dei dati biometrici potrà avvenire con riguardo a procedure di accesso da parte di soggetti autorizzati nel rispetto di **misure di garanzia** che il Garante è chiamato ad adottare, ma che ad oggi non sono state ancora elaborate.

Inoltre, sotto un profilo strettamente giuslavoristico, l'art. 4 della L. 300/1970 (c.d. **Statuto dei Lavoratori**) dispone che gli strumenti che consentono - anche solo potenzialmente - un controllo a distanza dell'attività lavorativa possono essere installati solo previo **accordo con le rappresentanze sindacali** o, in mancanza, previa **autorizzazione da parte dell'Ispettorato Territoriale del Lavoro** competente. Tale adempimento, secondo quanto previsto dal comma 2 dell'art. 4 dello Statuto dei Lavoratori, non viene invece richiesto con riferimento agli "*strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa*"[7] e agli "*strumenti di registrazione degli accessi e delle presenze*", tra i quali però non sembrerebbe rientrare anche un sistema di riconoscimento facciale deputato a tal fine.

Ciò, tenuto conto del fatto che il rispetto dei **principi di minimizzazione e proporzionalità** in merito all'utilizzo dei dati biometrici nell'ordinaria gestione del rapporto lavorativo, impone al datore di lavoro di adottare **misure utili allo scopo perseguito** – nel caso di specie la rilevazione delle presenze – ma il **meno invasive possibili** per i diritti degli interessati (*e.g.,* un *badge*).

L'Autorità ha quindi ordinato alle aziende soggette ai Provvedimenti di **sospendere l'uso dei sistemi biometrici** per controllare le presenze sul luogo di lavoro, **inibendo l'utilizzo dei dati** illecitamente raccolti e disponendone la **cancellazione**, irrogando anche delle **sanzioni pecuniarie amministrative**[8].

Cosa fare ora?

Tenuto conto dell'assenza di misure di garanzia ex art. 2-*septies* del Codice Privacy, e, nei casi oggetto dei Provvedimenti, di una idonea base di liceità per i trattamenti in oggetto, allo **stato l'ordinamento vigente non sembra lasciare molto margine** al trattamento di dati biometrici dei dipendenti per finalità di rilevazione della presenza in servizio e/o sul luogo di lavoro.

Ciò non di meno, in un'ottica di **mitigazione del rischio** e ai fini di una **maggiore *compliance***, le aziende pubbliche e private che intendano dotarsi di suddetti sistemi dovranno **escludere o quantomeno limitarne l'utilizzo** alle casistiche in cui risulti **indispensabile e debitamente comprovabile**, adottando le seguenti misure in materia di protezione dei dati personali e sotto il profilo giuslavoristico.

ADEMPIMENTI DATA PROTECTION

- condurre una **valutazione di impatto sulla protezione dei dati personali** ("**DPIA**") ai sensi dell'art. 35 del GDPR per vagliare i rischi per i diritti e libertà degli interessati[9] e, se del caso, procedere con una **consultazione preventiva** al Garante ai sensi dell'art. 36 del GDPR;

[7] Sul punto, si segnala che l'Ispettorato Nazionale del Lavoro, dopo qualche apertura iniziale, ha assunto una posizione abbastanza rigida, dichiarando che si può fare a meno dell'autorizzazione ministeriale e dell'accordo sindacale solo se lo strumento di lavoro è "*indispensabile*" al dipendente per svolgere la prestazione lavorativa, nel senso che il lavoratore, se dovesse essere privato di tale strumento, sarebbe impossibilitato a svolgere le sue mansioni.

[8] Nello specifico, con sanzioni rispettivamente di 70mila, 20mila, 6mila, 5mila e 2mila euro.

[9] I criteri per l'effettuazione di una DPIA, definiti dalle Linee-guida emanate dal WP 29 concernenti la valutazione d'impatto sulla protezione dei dati adottate da ultimo il 4 ottobre 2017 e reperibili qui, ricomprendono, tra gli altri (i) trattamenti valutativi o di *scoring*, compresa la profilazione; (ii) monitoraggio sistematico; (iii) trattamento di dati sensibili, giudiziari o di natura estremamente personale; (iv) trattamenti di dati personali su larga scala; (v) combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità; (vi) dati relativi a soggetti vulnerabili.

- adottare **misure tecniche e organizzative adeguate** a garantire la sicurezza del trattamento, nonché l'impiego di sistemi meno invasivi per i diritti e le libertà degli interessati[10] che perseguano le medesime finalità, come ad esempio i *badge*;
- designare tramite apposito ***Data Processing Agreement*** ("**DPA**") il **fornitore del sistema biometrico e/o di riconoscimento facciale**, quale responsabile del trattamento, valutando preventivamente l'adeguatezza delle misure tecniche e organizzative adottate dallo stesso;
- individuare la **base di liceità** più idonea al trattamento e integrare le **informative *privacy*** fornite ai dipendenti e collaboratori, dettagliando modalità di raccolta e di conservazione dei dati biometrici, nonché i diritti esercitabili con riferimento, in particolare, a tale tipologia di dati;
- integrare il **registro dei trattamenti**, conformemente a quanto previsto dall'art. 30 del GDPR.

ADEMPIMENTI GIUSLAVORISTICI

- sottoscrivere **accordi con le rappresentanze sindacali** o, in alternativa, ottenere **l'autorizzazione da parte dell'Ispettorato Territoriale del Lavoro competente** con riferimento al trattamento dei dati biometrici dei dipendenti, espletando le relative modalità e termini di conservazione;
- pena il divieto di utilizzo delle informazioni raccolte "*a tutti i fini connessi al rapporto di lavoro*" (inclusi i fini disciplinari), **informare i dipendenti** sulle **modalità d'uso degli strumenti** e sulle **modalità di effettuazione di eventuali controlli** (rivedendo le *policy* sugli strumenti di lavoro o, se non presenti, redigendole).

Possibili sanzioni

In caso di mancato rispetto delle prescrizioni del Garante e degli adempimenti di cui sopra, i datori di lavoro possono incorrere nelle seguenti violazioni della normativa giuslavoristica e dalla normativa in materia di protezione dei dati personali (a cui conseguono le relative sanzioni).

NORMATIVA GIUSLAVORISTICA

- la mancata sottoscrizione dell'accordo con le rappresentanze sindacali o il mancato ottenimento dell'autorizzazione da parte dell'Ispettorato Territoriale del Lavoro competente, in violazione dell'art. 4, comma 1 dello Statuto dei Lavoratori, comporta - salvo che il fatto non costituisca più grave reato – un'ammenda da euro 154 a euro 1.549 oppure l'arresto da 15 giorni a un anno, nonché il divieto di utilizzo delle informazioni raccolte "*a tutti i fini connessi al rapporto di lavoro*" (inclusi i fini disciplinari);
- qualora il datore di lavoro, in violazione delle garanzie di cui agli articoli 4 e 7 dello Statuto dei Lavoratori, non dovesse informare i dipendenti in merito alle modalità d'uso degli strumenti e alle modalità di effettuazione dei controlli (anche nel rispetto della normativa privacy), ne risulterebbe il divieto di utilizzare le informazioni raccolte "*a tutti i fini connessi al rapporto di lavoro*" (inclusi i fini disciplinari).

[10] Art. 5, par. 1 Regolamento (UE) 679/2016.

- nel caso in cui (i) non sia stato predisposto un DPA con il fornitore del sistema di riconoscimento facciale (art. 28 GDPR), (ii) non siano state adottate misure tecniche e organizzative adeguate a garantire un livello di sicurezza del trattamento adeguato al rischio connesso (art. 32 GDPR), (iii) non sia stata elaborata una DPIA relativa all'implementazione della nuova tecnologia (art. 35 GDPR), il datore di lavoro potrebbe incorrere in sanzioni amministrative pecuniarie **fino a 10 milioni di euro** o, se superiore, **fino a un massimo del 2% del fatturato mondiale totale annuo** dell'esercizio precedente, tenendo in considerazione vari fattori (es. natura della violazione, carattere doloso o colposo, grado di cooperazione con l'Autorità, eventuali precedenti violazioni);

- nel caso di (i) illiceità del trattamento per mancata sottoscrizione dell'accordo con le rappresentanze sindacali o il mancato ottenimento dell'autorizzazione da parte dell'Ispettorato Territoriale del Lavoro competente (art. 5, par. 1, lett. a), 6 e 88 GDPR), (ii) violazione dei principi di minimizzazione e proporzionalità del trattamento (art. 5 par. 1 lett. c) GDPR), nonché (iii) mancata predisposizione di un'informativa relativa al trattamento dei dati biometrici (art. 13 GDPR), il datore di lavoro potrebbe incorrere in sanzioni amministrative pecuniarie **fino a 20 milioni di euro** o, se superiore, **fino a un massimo del 4% del fatturato mondiale totale annuo** dell'esercizio precedente, tenendo in considerazione vari fattori (es. natura della violazione, carattere doloso o colposo, grado di cooperazione con l'Autorità, eventuali precedenti violazioni).

Osservazioni conclusive

Trattandosi di dati che consentono o confermano l'identificazione univoca di una persona fisica, il **divieto generale** di procedere al **trattamento dei dati biometrici**, affermato in linea di principio dal legislatore europeo, è concepito al fine di garantire la **protezione della dignità della persona**. In forza della loro peculiare natura e dei rischi a cui è soggetto il loro trattamento, infatti, appare necessario individuare, da parte dei vari soggetti coinvolti, le **misure di garanzia** più adeguate, anche in relazione alle finalità dello stesso.

Ad oggi, l'Autorità non ha predisposto delle vere e proprie **linee guida in materia di trattamento dei biometrici in ambito lavorativo**, ma anche dall'analisi dei Provvedimenti emerge che stia adottando un **approccio sempre più rigoroso** sul tema, tale per cui è raccomandabile **limitare il più possibile** l'utilizzo di detti dati in tale contesto, adottando in ogni caso **misure di sicurezza adeguate** alla natura "particolare" del trattamento, ivi incluse quelle tecniche di **cifratura e pseudonimizzazione**, di **minimizzazione e di accesso selettivo** ai dati, nonché tutti gli **adempimenti di *compliance*** con la normativa in materia di protezione dei dati personali e giuslavoristica sopraelencati.

Contatti

teamprivacy@lcalex.it

LCA Studio Legale
info@lcalex.it - www.lcalex.it

MILANO
Via della Moscova 18
20121 Milano

ROMA
Piazza del Popolo 18
00187 Roma

GENOVA
Via XX Settembre 31/6
16121 Genova

TREVISO
Via Sile 41
31056 Roncade (TV)

BRUXELLES
Place Poelaert 6
1000 Bruxelles

DUBAI
IAA Middle East Legale Consultants LLP
Liberty House, Office 514, DIFC

Member of ASLA