QuotidianoPIÙ

Consulenti Privacy

www.iconsulentiprivacy.it

Lunedì 01/07/2024 • 06:00

CASO RISOLTO CONTROLLO IN AZIENDA

Privacy: vietato l'uso del riconoscimento facciale per controllare le presenze

È lecito l'impiego di sistemi di **riconoscimento facciale** per monitorare le presenze dei dipendenti nel luogo di lavoro alla luce della disciplina in materia di protezione dei dati personali e dei provvedimenti del **Garante Privacy**? È questo l'interrogativo al quale cercheremo di rispondere illustrando un caso pratico.

di Fabio Pari - Avvocato - Resp. area legale www.skema.it

di Federica Greppi - Privacy Specialist

Una società, operante nel settore dello smaltimento dei rifiuti, collocava all'interno di un locale adiacente al sito produttivo un **dispositivo di riconoscimento facciale per rilevare le presenze dei dipendenti** sul luogo di lavoro.

L'installazione si era resa necessaria – a detta della società – per contrastare il fenomeno delle assenze e dei numerosi contenziosi avviati dai lavoratori per rivendicare presunte ore di **lavoro straordinario**, mai effettivamente svolte. Il fine, a prima vista, pareva del tutto legittimo.

Par fronte alla problematica descritta, la società si era affidata a un **fornitore di servizi per l'installazione e la manutenzione** di un dispositivo di riconoscimento dei dipendenti basato sulla **biometria del volto**. L'apparecchio, che registrava le presenze dei lavoratori previo riconoscimento facciale, conservava al suo interno le **impronte biometriche** dei volti dei dipendenti, elaborate dal dispositivo e protette da crittografia. Il dispositivo era poi collegato attraverso la rete internet ad un **software** tramite il quale era possibile **gestire i dati relativi alle timbrature** ovvero il codice identificativo del lavoratore, l'orario di ingresso e di uscita.

Il datore di lavoro aveva omesso di rivolgersi a un **consulente privacy**, nell'errata convinzione della liceità del trattamento e di aver installato un dispositivo conforme al Regolamento (EU) 2016/679 (GDPR), come specificato dalla scheda prodotto dell'apparecchio.

Cosa dice il GDPR a proposito di dati biometrici?

La vicenda in esame ruota intorno al concetto di "**dati biometrici**" definiti dall'art. 4, par. 1, n. 14 del GDPR 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". Ne sono un esempio il rilevamento delle impronte digitali, la scansione dell'iride o anche il riconoscimento facciale come nel nostro caso.

Stante la loro capacità di identificare in modo univoco e diretto l'individuo, i dati biometrici rientrano nella categoria dei **dati particolari**, il cui trattamento è di norma vietato, salvo che ricorra **una delle condizioni di liceità indicate dall'art. 9, par. 2, del GDPR**.

Con riguardo all'ambito lavorativo, il trattamento dei dati biometrici è consentito se "[…] è 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 (art. 9, par.2, lett. b), del GDPR).

È vero che le finalità di rilevazione delle presenze dei dipendenti e di verifica dell'osservanza dell'orario di lavoro possono rientrare nell'ambito di applicazione dell'art. 9, par. 2, lett. b), del GDPR; tuttavia, il **trattamento dei dati biometrici è consentito solo** "nella misura in cui sia **autorizzato dal diritto dell'Unione o degli Stati membri** […] in presenza di **garanzie appropriate** per i diritti fondamentali e gli interessi dell'interessato".

Secondo quanto disposto dall'art. 2-septies del decreto legislativo 30 giugno 2003, n.196 (Codice della privacy), i già menzionati **trattamenti possono essere effettuati conformemente alle misure di garanzia disposte dal Garante** (ai sensi dell'art. 9, par. 4, del GDPR). La mancanza di dette garanzie non consente allo stato attuale di effettuare un trattamento di dati biometrici dei dipendenti per finalità di rilevazione delle presenze.

Come ribadito in più occasioni dal Garante italiano della privacy, **l'utilizzo del dato biometrico** nel contesto della ordinaria gestione del rapporto di lavoro **viola i principi generali di minimizzazione e di proporzionalità del trattamento** (art. 5, par. 1, lett. c), del GDPR). Ciò significa che un tale trattamento è da ritenersi illecito, tenuto conto che la finalità di rilevazione delle presenze può essere raggiunta con mezzi meno intrusivi della sfera personale del lavoratore (ad esempio, il badge).

Le ulteriori violazioni del GDPR

Tornando al caso in esame, si evidenzia che il datore di lavoro aveva commesso ulteriori violazioni del GDPR quali: a) l'inadempimento dell'obbligo di rendere l'informativa specifica sul trattamento di dati biometrici; b) la mancata designazione del responsabile del trattamento; c) l'omessa valutazione di impatto; d) la mancata adozione di misure di sicurezza adeguate.

1. In ossequio al principio di trasparenza e al dovere di correttezza, il **datore di lavoro è tenuto ad informare i propri dipendenti e collaboratori** in merito alle caratteristiche dei trattamenti di dati personali effettuati in occasione del rapporto di lavoro in conformità all'art. 13 del GDPR. In concreto, il datore di lavoro avrebbe dovuto rendere ai lavoratori **una specifica informativa sul trattamento di dati biometrici** tramite riconoscimento facciale, ciò che nel caso specifico non si è verificato.
2. Altra violazione è la **mancata designazione del responsabile del trattamento**. In qualità di titolare del trattamento, il datore di lavoro ha la possibilità di avvalersi di un responsabile, al quale impartisce specifiche istruzioni per il compimento di alcune attività di trattamento (art. 28 del GDPR). Nel caso specifico, mancava l'atto di nomina a responsabile nei confronti del fornitore installatore del dispositivo, che aveva accesso al software di gestione delle presenze per fini di assistenza e manutenzione.
3. L'art 35 del GDPR impone al titolare del trattamento di effettuare una valutazione di impatto, (DPIA) prima dell'inizio del trattamento, ogniqualvolta "**l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento **possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche**". In proposito, le Linee guida del WP 248rev.01 del 4.4.2017 (Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679) individuano tra i criteri in presenza dei quali la valutazione di impatto è obbligatoria: i **trattamenti di "dati sensibili**" nei quali sono compresi i dati biometrici, i trattamenti **effettuati nei confronti di interessati "vulnerabili"** (ad es. i lavoratori in quanto soggetti deboli in un rapporto di lavoro) e i trattamenti che realizzano un "**uso innovativo** o l'**applicazione di nuove soluzioni tecnologiche od organizzative**". Stante la compresenza di tali criteri, il datore di lavoro avrebbe dovuto effettuare una valutazione d'impatto, ai sensi dell'art. 35 del GDPR.
4. Ai sensi dell'art.32 del GDPR, il titolare del trattamento è tenuto a mettere in atto "**misure tecniche e organizzative adeguate** a garantire un livello di sicurezza adeguato al rischio", tenuto conto "dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche". Nel caso di specie, risultava che il dispositivo era accessibile tramite le medesime credenziali di autenticazione riportate nel manuale di utilizzo che peraltro non erano mai state modificate nel corso del tempo. Ciò significa che chiunque poteva agevolmente accedere al dispositivo e prendere visione dei dati relativi alle timbrature e all'anagrafica degli utenti.