LABOR Il lavoro nel diritto

Pacini Giuridica

Violazione della normativa in tema di privacy e riservatezza: profili ricostruttivi sul divieto di riconoscimento facciale dei dipendenti ai fini della verifica delle presenze sul posto di lavoro

di G. M. Marsico - *13 Maggio 2024*

Il Garante Privacy, con i provvedimenti in analisi (nn. 105, 106, 107, 108 e 109 del 22 febbraio 2024), ha statuito che il riconoscimento facciale utilizzato al fine di verificare le presenze dei dipendenti sul posto di lavoro dei lavoratori viola la normativa a tutela della privacy dei dipendenti, ed ha quindi sanzionato cinque diverse società per violazione del GDPR, sotto molteplici profili.

In particolare, è stata accertata preliminarmente la violazione dell'art. 5, par. 1, lett. a) e 9 del Regolamento, in relazione ai trattamenti di dati dei citati dipendenti.

Nei diversi casi sottoposti all'analisi dell'Autorità analizzati si era realizzato, in concreto, un trattamento di dati biometrici in due distinti momenti.

Il primo che viene in rilievo è quello relativo alla fase di registrazione (c.d. *enrolment*), consistente nella acquisizione delle caratteristiche biometriche dell'interessato (caratteristiche del volto, nel caso di specie; v. punti 6.1 e 6.2 dell'allegato A al provvedimento del Garante del 12 novembre 2014, n. 513)

Il secondo è quello che attiene alla fase di riconoscimento biometrico, all'atto della rilevazione delle presenze (v. anche punto 6.3 dell'allegato A al citato provvedimento).

Dunque, si è ribadito che, anche in caso di estrazione del c.d. *template*, ad avviso del Garante, tramite il riconoscimento facciale dei lavoratori, si sarebbe realizzato un effettivo trattamento di dati biometrici, con conseguente applicazione della specifica disciplina prevista dal GDPR (L. Greco, A. Mantelero, *Industria 4.0, robotica e privacy-by-design*, in *Diritto dell'Informazione e dell'Informatica*, n. 6, 2018, 876 e ss. Sui sistemi di autenticazione attraverso dati biometrici, cfr. B. Rubis, *Sistemi di autenticazione mediante l'utilizzo di dati biometrici*, in *Diritto dell'Informazione e dell'Informatica*, 2023).

In proposito, in base alla normativa posta in materia di protezione dei dati personali, il trattamento di dati biometrici (di regola vietato ai sensi dell'art. 9, par. 1 del Regolamento) è consentito esclusivamente qualora ricorra una delle condizioni indicate dall'art. 9, par. 2 del Regolamento.

Tanto rilevato in via generale, occorre premettere brevi cenni in fatto, in particolare e per semplicità, sul provvedimento n. 105, il cui contenuto in punto di diritto risulta sovrapponibile agli altri provvedimento in commento.

In data 24 ottobre 2022, alcuni dipendenti di L'Igiene Urbana Evolution s.r.l., hanno presentato reclamo all'Autorità lamentando che, a partire dal mese di febbraio 2022, al fine di accedere al cantiere situato in Ardea, ove si svolge l'attività lavorativa dei dipendenti, e di accertare la presenza degli stessi sul luogo di lavoro, era necessario utilizzare un rilevatore biometrico, basato sul riconoscimento facciale. In base alla documentazione, anche fotografica, allegata ai reclami il trattamento sarebbe stato effettuato mediante il dispositivo "*Face Deep 3 – Smart Face Recognition System"*, prodotto da Anviz Global.

Secondo quanto lamentato i trattamenti di dati personali biometrici sarebbero "illegittimi", tenuto anche conto che la finalità degli stessi "potrebbe essere egualmente raggiunta con mezzi meno invasivi della sfera personale del lavoratore".

L'Autorità ha delegato il Nucleo speciale privacy e frodi tecnologiche della Guardia di finanza ad effettuare accertamenti ispettivi ai sensi degli artt. 157 (Richiesta di informazioni e di esibizione di documenti) e 158 (Accertamenti) del Codice. In data 19 gennaio 2023, il Nucleo, unitamente a personale dell'Autorità, si è recato presso il cantiere sito in Ardea, dove ha acquisito a verbale le seguenti dichiarazioni dalle quali risulta che: all'interno del sito industriale di rimessaggio operano le seguenti società: L'Igiene Urbana Evolution s.r.l., Airone società consortile a r.l., Blue Work s.r.l., che operano come ATI per la gestione dei rifiuti del Comune di Ardea"; all'interno di un locale adiacente al parco automezzi è presente un dispositivo di riconoscimento dei dipendenti basato sulla biometria del volto (A. Trojsi, *Il diritto del lavoratore alla protezione dei dati personali*, Torino, 2013, 108).

Il sistema viene utilizzato per la rilevazione delle presenze, dai circa 63 dipendenti delle società che operano nel cantiere più eventuali stagionali o sostituti temporanei"; la fase di registrazione dei dipendenti, è stata effettuata mediante l'inserimento del codice dipendente (ID) associato al nominativo, sulla base di un elenco fornito dalla società stessa. Una volta inserito tale ID avveniva il riconoscimento del volto del dipendente e il sistema convalidava la registrazione".

Accedendo con le credenziali di *Admin*, così come riportate nel manuale di utilizzo e non modificate nell'installazione, sono stati esportati i dati relativi alle timbrature e all'anagrafica degli utenti ed è stato effettuato il *back up* del *db interno*; si è rilevato come sia effettuato l'accesso all'applicativo JuniorWeb "tramite cui vengono gestite le presenze dei dipendenti, così come registrate tramite il dispositivo di riconoscimento facciale. Sono stati effettuati gli export delle anagrafiche, comprendenti anche i dipendenti licenziati, ed è stato verificato che il sistema riporta l'indicazione di 3 ulteriori società (DMT, IGNEVO, UNICA srl) e di 17 ulteriori centri di costo".

In data 26 gennaio 2023, inoltre, nel corso dell'accertamento ispettivo effettuato presso la sede amministrativa di L'igiene Urbana Evolution s.r.l., la Società ha dichiarato che: "l'Associazione temporanea di imprese (ATI) è stata costituita nel gennaio 2020.

Attualmente l'ATI è composta dalle società: l'Igiene Urbana Evolution e Blu Work. Nel marzo 2021, ai soli fini della gestione operativa della commessa, le società L'Igiene Urbana Evolution e Blu Work hanno costituito la Airone società consortile a r.l.

L'apparecchio biometrico di rilevamento presenze in Ardea è stato installato dalla capogruppo anche alla luce di numerosi procedimenti disciplinari relativi a ritardi, assenze, interruzioni e abbandoni del servizio nonché in virtù dei numerosi contenziosi e sentenze di condanna collegati a rivendicazioni di compensi di lavoro straordinario, tenuto conto che il servizio di raccolta e trasporto rifiuti è un servizio pubblico essenziale.

Il sistema si è anche ritenuto necessario in quanto tutti i dipendenti del cantiere di Ardea sono stati assunti in forza di clausola sociale" (si veda C. Colosimo, *La moderna declinazione del potere di controllo*, in AA.VV., *Diritti e doveri nel rapporto di lavoro*, Milano, 2018, 67).

Tuttavia, come da Ispettorato Nazionale del Lavoro, Circolare n. 5/2018, 19 febbraio 2018, 5, si deve ritenere che il trattamento dei dati biometrici sia legittimo in assenza dell'accordo sindacale, quando la finalità unicamente perseguita consiste nell'accesso ad aree riservate o nell'utilizzo di determinati strumenti considerati pericolosi(per maggiori approfondimenti si veda I. Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in *Labour & Law Issues*, n. 2, 2016, 3 ss.).

Il 13 settembre 2023, l'Ufficio del Garante ha effettuato, ai sensi dell'art. 166, comma 5, del Codice, la notificazione alla Società delle presunte violazioni del Regolamento riscontrate, con riferimento agli artt. 5, par. 1, lett. a), 9, par. 2, 13, 28, 30, 32 e 35 del Regolamento.

Con memorie difensive inviate in data 13 ottobre 2023, la Società ha dichiarato che: a. la Società ha riscontrato "nel corso del 2021 un pesante aggravamento del fenomeno dell'assenteismo, segnatamente accompagnato da timbrature fraudolente che attestavano la presenza in servizio di dipendenti che, in realtà, non prestavano regolarmente la loro prestazione. Conseguentemente, si è agito per richiedere il riconoscimento di differenze retributive per presunte ore di lavoro straordinario prestato ma che, invero, la società non riteneva fossero mai state effettivamente svolte. I procedimenti, inoltre, hanno avuto esiti negativi proprio in virtù della circostanza per cui la medesima società era impossibilitata a verificare con certezza l'effettivo orario di lavoro prestato dai ricorrenti (in quanto venivano utilizzati fogli presenze cartacei).

Sempre sul piano fattuale si è rilevato che gli ordinari strumenti di contrasto adottati a tale fine, si sono dimostrati del tutto inefficaci (A. Levi, *Il controllo informatico sull'attività del lavoratore*, Torino, 2013, 144; M. Soffientini, *Sistema di videosorveglianza in azienda: progettazione ed errori comuni da evitare*, in *Diritto e Pratica del Lavoro*, n. 5, 2023, 323).

L'adozione di un sistema di rilevazione delle presenze mediante riconoscimento facciale è stata realizzata rivolgendosi alla [società fornitrice dei dispositivi], che commercializza un sistema implementato da un'azienda leader sul mercato (Anviz Global), il cui applicativo (Face Deep 3 – Smart Face Recognition System) veniva presentato come uno strumento pienamente coerente con i vincoli derivanti dal rispetto della normativa a tutela della protezione dei dati personali dei lavoratori.

Occorre precisare che, nel verbale del 19/01/2023, in relazione al contenuto del back-up del DB interno al dispositivo acquisito dagli ispettori, l'indicazione "timbrature ed anagrafiche utenti" deve, invero, intendersi riferita ad un mero codice numerico (corrispondente ad ogni lavoratore) correlato alla data e all'orario di timbratura. […] i *template* biometrici cifrati, acquisti in fase di *enrollment*], risultavano associati ai suddetti codici numerici, senza alcuna memorizzazione nel dispositivo del nome e cognome degli interessati".

Particolare attenzione occorre prestare al rilievo, sicuramente fondato, sulla non robustezza della password per l'accesso all'applicativo del dispositivo"; la società ha ribadito, a sua difesa, come si sia comunque sempre garantita al personale la possibilità di non utilizzare l'applicativo per il riconoscimento facciale, sostituendolo con i fogli presenza […], come in caso, ad esempio, di malfunzionamento o non attivazione dei dispositivi.

All'esito dell'esame delle dichiarazioni rese all'Autorità nel corso del procedimento nonché della documentazione acquisita, risulta che la Società, in qualità di titolare, ha effettuato alcune operazioni di trattamento, riferite ai reclamanti, che risultano non conformi alla disciplina in materia di protezione dei dati personali. In proposito si evidenzia che, salvo che il fatto non costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante".

Nel merito, all'esito dell'attività istruttoria, è stato accertato che la Società ha utilizzato un sistema biometrico, basato sul riconoscimento facciale, a partire dal mese di dicembre 2021 (data in cui è stato attivato il sistema, secondo quanto dichiarato dalla Società; tuttavia la stessa non ha chiarito in quale data fossero iniziate le attività di registrazione dei dipendenti con conseguente trattamento di dati) e fino al mese di gennaio 2023, data in cui il sistema è stato disattivato "a titolo cautelativo" a seguito dell'avvio dell'attività di accertamento da parte dell'Autorità (R. Krause, *The protection of employees'right to privacy: the German legal system*, in C. Pisani, G. Proia, A. Topo (a cura di), *Privacy e lavoro: la circolazione dei dati personali e i controlli nel rapporto di lavoro*, Milano, 2022, 250).

L'utilizzo del sistema biometrico, finalizzato alla rilevazione della presenza in servizio dei dipendenti, è stato determinato, in base a quanto dichiarato, dal moltiplicarsi di fenomeni di "assenteismo" e di vertenze avviate nei confronti della Società stessa da parte dei lavoratori relative "a rivendicazioni di compensi di lavoro straordinario".

Inoltre, l'adozione del sistema biometrico, secondo quanto dichiarato dalla Società, si sarebbe reso necessario anche in forza del fatto che "tutti i dipendenti del cantiere di Ardea sono stati assunti in forza di clausola sociale, con conseguente impossibilità per il datore di scegliere i contraenti del contratto di lavoro.

Il trattamento ha riguardato un numero significativo di interessati, considerato che, nel corso degli accertamenti, è emerso che la Società ha utilizzato il medesimo tipo di rilevatore biometrico, non solo presso il cantiere di Ardea, bensì anche presso ulteriori 9 siti, presso i quali svolge la propria attività. In particolare, in base all'esame del "prospetto riguardante le diverse sedi di installazione dei dispositivi" fornito dalla Società, comprensivo del numero di propri

dipendenti impiegati presso ciascuna sede, emerge che il trattamento ha interessato un totale di 288 lavoratori.

Anche sottraendo i 12 lavoratori del sito presso il Comune di Ravello, il cui dispositivo sarebbe stato "montato [ma] mai andato in funzione", come indicato nel prospetto (senza tuttavia specificare se sia stata effettuata o meno la raccolta dei dati, che è comunque una operazione di trattamento), si tratterebbe in totale di 276 dipendenti, ossia un numero comunque significativo di interessati coinvolti dal trattamento di dati biometrici.

Diversamente da quanto sostenuto nelle memorie difensive, inoltre, la Società nel corso del procedimento non ha indicato né documentato l'esistenza di ritenute "posizioni duplicate", considerate le quali il numero complessivo di interessati dalla rilevazione biometrica ammonterebbe invece a 218 dipendenti, e in ogni caso anche tale numero appare significativo.

Si osserva che, come chiarito dall'Autorità, vi è trattamento di dati biometrici sia nella fase di registrazione (c.d. *enrolment*), consistente nella acquisizione delle caratteristiche biometriche dell'interessato (caratteristiche del volto, nel caso di specie; v. punti 6.1 e 6.2 dell'allegato A al provvedimento del Garante del 12 novembre 2014, n. 513, in www.garanteprivacy.it, doc. web n. 3556992), sia nella fase di riconoscimento biometrico, all'atto della rilevazione delle presenze (v. anche punto 6.3 dell'allegato A al citato provvedimento).

Pertanto, anche in caso di estrazione del c.d. *template*, vi è trattamento di dati biometrici, con conseguente applicazione della specifica disciplina prevista dall'ordinamento.

In proposito, in base alla normativa posta in materia di protezione dei dati personali, il trattamento di dati biometrici (di regola vietato ai sensi dell'art. 9, par. 1 del Regolamento) è consentito esclusivamente qualora ricorra una delle condizioni indicate dall'art. 9, par. 2 del Regolamento e, con riguardo ai trattamenti effettuati in ambito lavorativo, solo quando il trattamento sia "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 Regolamento; v. anche: art. 88, par. 1 e cons. 51-53 del Regolamento).

Il datore di lavoro, inoltre, è tenuto ad applicare i principi generali del trattamento, in particolare quelli di liceità, correttezza e trasparenza, minimizzazione, integrità e riservatezza dei dati (art. 5, par. 1, lett. a), c) e f) del Regolamento).

In applicazione di tali disposizioni, sebbene nel contesto lavorativo le finalità di rilevazione delle presenze dei dipendenti e di verifica dell'osservanza dell'orario di lavoro possano rientrare nell'ambito di applicazione dell'art. 9, par. 2, lett. b) del Regolamento, 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" (art. 9, par. 2, lett. b), e cons. nn. 51-53 del Regolamento).

Tenuto anche conto di quanto previsto dall'art. 2-septies del Codice (Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute), in base al quale i predetti trattamenti possono essere effettuati conformemente alle misure di garanzia disposte dal Garante (ai sensi dell'art. 9, par. 4, del Regolamento), allo stato, secondo il Garante, l'ordinamento vigente non consente il trattamento di dati biometrici dei dipendenti per finalità di rilevazione della presenza in servizio (L. Torsello, *Persona e lavoro nel sistema CEDU. Diritti fondamentali e tutela sociale nell'ordinamento multilivello*, Cacucci, 2019, spec. sub 17 ss. V. anche, S. Sciarra, *Di fronte all'Europa. Passato e presente del diritto del lavoro,* in *CSDLE*, Int, n. 12/2003; *La costituzionalizzazione dell'Europa Sociale. Diritti fondamentali e procedure di soft law,* in *CSDLE*, Int, n.16/2003; B. Caruso, *Il diritto del lavoro tra hard law e soft law: nuove funzioni e nuove tecniche normative,* in *CSDLE*, It, n. 39/2005; A. Alaimo, *Il diritto al lavoro fra Costituzione nazionale e Carte europee dei diritti: un diritto "aperto" e "multilivello", CSDLE*, Int, n. 60/2008; L. Zoppoli, *Valori, diritti e lavori flessibili: storicità, bilanciamento, declinabilità, negoziabilità,* in *CSDLE*, It, n. 400/2019, 8 ss.).

Ciò è stato ribadito dal Garante medesimo con i provvedimenti n. 369, del 10 novembre 2022 (doc. web n. 9832838) e n. 16, del 14 gennaio 2021.

L'utilizzo del dato biometrico nel contesto dell'ordinaria gestione del rapporto di lavoro (quale è l'attività di rilevazione delle presenze), al dichiarato fine di far fronte ad illeciti disciplinari, contenziosi legati alla corresponsione del compenso per il lavoro straordinario nonché a causa della presenza di personale presso il cantiere ove si è svolta l'attività di accertamento assunto mediante l'applicazione della c.d. clausola sociale (sebbene tale ultima motivazione non sia conferente, tenuto altresì conto che non sono state rese note le motivazioni in forza delle quali il sistema biometrico è stato adottato anche presso ulteriori 9 siti gestiti dalla Società), non è, secondo l'Autorità, dunque conforme ai principi di minimizzazione e proporzionalità del trattamento (art. 5, par. 1, lett. c) del Regolamento).

Invero, la Società, secondo il Garante, non avrebbe illustrato (né documentato nel corso del procedimento) quali "ordinari strumenti di contrasto" fossero stati in concreto adottati e si fossero rivelati "del tutto inefficaci", al fine di poter contabilizzare le effettive ore di lavoro prestate e di accertare la presenza dei lavoratori sul luogo di lavoro avrebbero potuto essere adottate misure utili allo scopo ma meno invasive per i diritti degli interessati (es. controlli automatici mediante badge, verifiche dirette, etc.).

La valutazione di proporzionalità del trattamento di dati biometrici consistenti nel riconoscimento facciale avrebbe dovuto tener conto, inoltre, dei rischi per i diritti e le libertà degli interessati connessi all'uso di tale particolare tecnologia biometrica così come è stato riconosciuto sia dall'ordinamento nazionale che in ambito europeo: v. d.l. 10/5/2023, n. 51, conv. in l. 3/7/2023, n. 87, che con l'art. 8-ter 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", ciò al fine di "disciplinare conformemente i requisiti di ammissibilità, le condizioni e le garanzie relativi all'impiego di sistemi di riconoscimento facciale nel rispetto del principio di proporzionalità previsto dall'articolo 52 della Carta dei diritti fondamentali dell'Unione europea".

Merita anche richiamare in proposito: European data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, adottate il 26/7/2023, spec. punti 17, 34 e 35 sui rischi del riconoscimento facciale; Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate il 29 gennaio 2020, spec. punti 4 e 73; si veda altresì il Provv. del 10 febbraio 2022, n. 50, doc. web n. 9751362, adottato, seppure in un diverso contesto, in materia di riconoscimento facciale).

Infine, secondo il Garante, la circostanza che il produttore e il fornitore dei dispositivi di riconoscimento facciale (soggetti che in ogni caso devono tener conto del diritto alla protezione dei dati: v. cons. 78 del Regolamento) avessero prodotto una "dichiarazione e certificazione di conformità dell'apparato biometrico, in cui veniva dichiarato che il dispositivo era pienamente conforme al GDPR", non può far venir meno la responsabilità della Società, considerato che il titolare del trattamento, alla luce di quanto stabilito dall'art. 5, par. 2, del Regolamento, in base al c.d. principio di responsabilizzazione, "è competente per il rispetto dei principi generali del trattamento e in grado di comprovarlo", con riguardo agli obblighi che gravano sullo stesso (art. 24 del Regolamento).

L'Autorità con i provvedimenti *de quibus* ha ribadito i criteri di legittimazione e i principi applicabili al trattamento di dati biometrici nell'ambito del rapporto di lavoro, pubblicando sul proprio sito istituzionale le decisioni adottate in materia.

Pertanto, il titolare del trattamento, prima di procedere all'utilizzo di dispositivi realizzati da terzi, avrebbe dovuto verificare la conformità dei relativi trattamenti ai principi applicabili.

Da ultimo, si osserva che la possibilità di utilizzare i fogli firma non era alternativa, come dedotto dalla Società, all'uso del dispositivo di riconoscimento facciale, posto che i dipendenti potevano ricorrervi, in base a quanto emerge dalla documentazione presente in atti, solo in caso di malfunzionamento dei dispositivi biometrici.

Tuttavia, anche qualora un sistema di rilevazione non biometrico fosse stato messo a disposizione dei lavoratori in alternativa a quello biometrico, i trattamenti di dati effettuati non sarebbero stati conformi alle disposizioni in materia di protezione dei dati personali nei termini su esposti, e in concreto sarebbero risultati non necessari rispetto alla dichiarata finalità di ovviare ai problemi legati proprio all'uso dei fogli firma per attestare la presenza sul luogo di lavoro.

Pertanto, il trattamento di dati biometrici dei propri dipendenti effettuato dalla Società risulta pertanto essere stato effettuato in assenza di un'idonea base giuridica, in violazione degli artt. 5, par. 1, lett. a) e 9 del Regolamento.

In base all'art. 35 del Regolamento, infatti, in relazione a trattamenti che prevedono "l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, [tali da] presentare un rischio elevato per i diritti e le libertà delle persone fisiche", il titolare è tenuto ad effettuare una valutazione dell'impatto sulla protezione dei dati personali prima dell'inizio dei trattamenti previsti. In proposito, le "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 il titolare del trattamento è tenuto ad effettuare una valutazione di impatto,

rilevanti nel caso di specie, il trattamento di "dati sensibili", tra i quali sono compresi i dati biometrici, il trattamento effettuato nei confronti di interessati "vulnerabili" nonché i trattamenti che realizzano un "uso innovativo o l'applicazione di nuove soluzioni tecnologiche od organizzative".

Ulteriori indicazioni utili per la ricostruzione della *querelle* sottoposta all'attenzione del Garante sono state fornite in proposito con il provvedimento del Garante dell'11 ottobre 2018, n. 467 ("Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679", in G.U., S. G. n. 269 del 19/11/2018, spec. n 6 e 7), sebbene riferito a trattamenti transfrontalieri (M. D'Antona, *Il diritto al lavoro nella Costituzione e nell'ordinamento comunitario*, in M. D'Antona, Opere, Giuffrè, 2000, I, 268; F. Borgogelli – S. Giubboni, *Il lavoro come diritto sociale. Appunti per una voce di enciclopedia*, in *RDSS*, 2006, 327; S. Giubboni, *Il primo dei diritti sociali. Riflessioni sul diritto al lavoro tra Costituzione italiana e ordinamento europeo*, in *CSDLE*, Int, n. 46/2006).

Pur avendo adottato un sistema di autenticazione biometrica per finalità di rilevazione delle presenze dei propri dipendenti presso tutti i siti dove questi operano, la Società, secondo il Garante, non avrebbe però provveduto a effettuare una valutazione di impatto, prima dell'inizio dei trattamenti stessi, in violazione pertanto, nei termini su esposti, dell'art. 35, par. 1 del Regolamento.

Per i suesposti motivi, l'Autorità ritiene che, nel caso concreto, le dichiarazioni, la documentazione e le ricostruzioni fornite dal titolare del trattamento, nel corso dell'istruttoria, non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e che risultano pertanto inidonee a consentire l'archiviazione del presente procedimento, non ricorrendo peraltro alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Il trattamento dei dati personali effettuato dalla Società e segnatamente il trattamento di dati biometrici – riconoscimento facciale – riferiti ai propri dipendenti e a quelli di altre società, per finalità

di rilevazione delle presenze, risulta infatti illecito, nei termini su esposti, in relazione agli artt. 5, par. 1, lett. a), 9, 13, 28, 30, 32 e 35 del Regolamento.

La violazione, accertata nei termini di cui in motivazione, non può essere considerata "minore", tenuto conto della natura della violazione che ha riguardato i principi generali e le condizioni di liceità del trattamento di dati particolari nonché della gravità della violazione stessa, del grado di responsabilità e della maniera in cui l'autorità di controllo ha preso conoscenza della violazione. L'Autorità prende comunque atto che, secondo quanto dichiarato sotto propria responsabilità, la Società ha provveduto a sospendere le operazioni di trattamento dei dati biometrici dopo l'avvio dell'attività ispettiva ed ha individuato una "procedura per la dismissione dei dispositivi biometrici"

la quale prevede, tra l'altro, che al termine del procedimento avviato dal Garante, i dati conservati sui dispositivi siano cancellati.

Pertanto, secondo l'Autorità, in considerazione dei poteri correttivi attribuiti dall'art. 58, par. 2 del Regolamento, il procedimento si definisce con la sola applicazione di una sanzione amministrativa pecuniaria, ai sensi dell'art. 83 del Regolamento, commisurata alle circostanze del caso concreto (art. 58, par. 2, lett. i) Regolamento).

All'esito del procedimento, dunque, risulta che le società abbiano violato gli artt. 5, par. 1, lett. a), 9, 13, 28, 30, 32 e 35 del Regolamento. Per la violazione delle predette disposizioni è prevista l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 4, lett. a) e par. 5, lett. a) e b) del Regolamento, mediante adozione di un'ordinanza ingiunzione.

Il Garante, ritenuto di dover applicare il paragrafo 3 dell'art. 83 del Regolamento laddove prevede che "Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento […] viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave", l'importo totale della sanzione è calcolato in modo da non superare il massimo edittale previsto dal medesimo art. 83, par. 5.

Con riferimento agli elementi elencati dall'art. 83, par. 2 del Regolamento ai fini della applicazione della sanzione amministrativa pecuniaria e la relativa quantificazione, tenuto conto che la sanzione deve "in ogni singolo caso essere effettiva, proporzionata e dissuasiva" (art. 83, par. 1 del Regolamento), si rappresenta che il Garante, nei casi di specie, ha valutato le seguenti circostanze: a) in relazione alla natura, gravità e durata della violazione, è stata considerata, a sfavore della Società, la natura della violazione che ha riguardato i principi generali e le condizioni di liceità del trattamento e il trattamento di dati particolari biometrici utilizzando la tecnologia del riconoscimento facciale; b) è stata altresì considerata, a sfavore della Società, la durata della violazione che si è protratta per più di un anno e il numero significativo degli interessati coinvolti; c) con riferimento al carattere doloso o colposo della violazione e al grado di responsabilità del titolare, è stata presa in considerazione la condotta della Società e il grado di responsabilità della stessa che non si è conformata alla disciplina in materia di protezione dei dati relativamente a una pluralità di disposizioni; d) a favore della Società, si è tenuto conto della cooperazione con l'Autorità di controllo e della decisione di sospendere le attività di trattamento dopo l'inizio delle attività ispettive.

Si ritiene inoltre che assumano rilevanza nel caso di specie, tenuto conto dei richiamati principi di effettività, proporzionalità e dissuasività ai quali l'Autorità deve attenersi nella determinazione dell'ammontare della sanzione (art. 83, par. 1, del Regolamento), in primo luogo le condizioni economiche del contravventore, determinate in base ai ricavi conseguiti dalla Società con riferimento al bilancio ordinario d'esercizio per l'anno 2022.

Da ultimo il Garante ha considerato l'entità delle sanzioni irrogate in casi analoghi. Alla luce degli elementi sopra indicati e delle valutazioni effettuate, ha ritenuto, nel caso di specie, di applicare nei confronti delle società. la sanzione amministrativa del pagamento di una somma di denaro.

In tale quadro si ritiene, altresì, in considerazione della tipologia delle violazioni accertate che hanno riguardato i principi generali e le condizioni di liceità del trattamento, che ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n.

1/2019, si debba procedere alla pubblicazione del presente provvedimento sul sito Internet del Garante. Si ritiene, altresì, che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

In conclusione, dunque, in base alla normativa posta in materia di protezione dei dati personali, il trattamento di dati biometrici (di regola vietato ai sensi dell'art. 9, par. 1 del Regolamento) è consentito esclusivamente qualora ricorra una delle condizioni indicate dall'art. 9, par. 2 del Regolamento.

Ovvero, con riguardo ai trattamenti effettuati in ambito lavorativo, solo quando il trattamento congiuntamente:

- sia 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
- 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 (v. art. 9, par. 2, lett. b), e art. 88, par. 1 e cons. 51-53 del Regolamento).

Il datore di lavoro, inoltre, è tenuto ad applicare i principi generali del trattamento, in particolare quelli di liceità, correttezza e trasparenza, minimizzazione, integrità e riservatezza dei dati (art. 5, par. 1, lett. a), c) e f) del Regolamento).

Tenuto anche conto di quanto previsto dall'art. 2-septies del Codice (Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute), in base al quale i predetti trattamenti possono essere effettuati conformemente alle misure di garanzia disposte dal Garante (ai sensi dell'art. 9, par. 4, del Regolamento), allo stato attuale il nostro ordinamento non consente il trattamento di dati biometrici dei dipendenti per finalità di rilevazione della presenza in servizio.

Ciò era già stato ribadito dal Garante con i provvedimenti n. 369/2022 e n. 16/2021 (M. Militello, *Principio di uguaglianza* cit., 14 ss. Sull'art. 21 della Carta di Nizza, F. Guarriello, *Il principio di non discriminazione nel lavoro*, in *Carta dei diritti fondamentali dell'Unione europea* cit., 2017, 426 ss.).

L'utilizzo del dato biometrico nel contesto dell'ordinaria gestione del rapporto di lavoro, come l'attività di rilevazione delle presenze, al dichiarato fine di far fronte ad illeciti disciplinari, contenziosi legati alla corresponsione del compenso per il lavoro straordinario, nonché a causa della presenza di personale presso il cantiere ove si è svolta l'attività di accertamento, non è dunque conforme ai principi di minimizzazione e proporzionalità del trattamento (art. 5, par. 1, lett. c) del Regolamento).

In conclusione, le aziende, ad avviso del Garante, avrebbero dovuto più opportunamente utilizzare sistemi meno invasivi per controllare la presenza dei propri dipendenti e collaboratori sul luogo di lavoro (come ad es. il badge).

Dall'attività ispettiva del Garante, nei casi analizzati, sono inoltre emerse ulteriori violazioni da parte delle società.

In particolare, l'Autorità 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, e violando pertanto l'art. 32 del GDPR.

Le aziende, poi, non avevano fornito una informativa chiara e dettagliata ai lavoratori, in violazione dell'art. 13 del Regolamento, né avevano effettuato la valutazione d'impatto prevista dalla normativa privacy, violando altresì l'art. 35 del GDPR (Cfr. P. Trimarchi, *Rischio e responsabilità oggettiva*, Milano, 1961, pp. 9-10).

Infine, in base a quanto stabilito dall'art. 30 del Regolamento, all'interno del registro delle attività di trattamento svolte dal titolare, quest'ultimo, sotto la propria responsabilità, è sempre tenuto a indicare le categorie di dati personali oggetto di trattamento (art. 30, par. 1, lett. c) del Regolamento): nel caso concreto, è emerso invece che il registro delle operazioni di trattamento non indicava i dati biometrici tra i tipi di dati trattati dal titolare, violando ulteriormente il citato disposto del GDPR.

Come sottolineato dal Garante, in un'ottica di adeguatezza e proporzionalità, per il controllo delle presenze di dipendenti e collaboratori sul luogo di lavoro, sarebbe più opportuno utilizzare sistemi meno invasivi, come ad esempio controlli automatici tramite badge o verifiche dirette.

Ulteriori violazioni possono riguardare poi la mancata adozione di specifiche misure di sicurezza, necessarie per la rilevazione biometrica. Le aziende, infatti, devono fornire ai lavoratori e alle lavoratrici informative chiare e dettagliate ed effettuare la valutazione d'impatto prevista dalla normativa sulla privacy.

Giuseppe Maria Marsico, dottorando di ricerca in diritto privato e dell'economia e funzionario giuridico-economico-finanziario

Visualizza i documenti: Garante Privacy, provvedimento 22 febbraio 2024, n. 105; Garante Privacy, provvedimento 22 febbraio 2024, n. 106; Garante Privacy, provvedimento 22 febbraio 2024, n. 107; Garante Privacy, provvedimento 22 febbraio 2024, n. 108; Garante Privacy, provvedimento 22 febbraio 2024, n. 109