



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Provvedimento del 22 febbraio 2024 [9995762]

VEDI ANCHE [Newsletter del 28 marzo 2024](#)

[doc. web n. 9995762]

Provvedimento del 22 febbraio 2024

Registro dei provvedimenti
n. 108 del 22 febbraio 2024

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzone, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti e il cons. Fabio Mattei, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (di seguito, "Regolamento");

VISTO il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, di seguito "Codice");

ESAMINATA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il dott. Agostino Ghiglia;

PREMESSO

1. I reclami presentati.

In data 24 ottobre 2022, alcuni dipendenti di L'Igiene Urbana Evolution s.r.l. e Airone società consortile a 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, del tipo "Face Deep 3 – Smart Face Recognition System", prodotto da Anviz Global.

2. L'attività istruttoria effettuata.

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.

Nel corso di tale attività delegata, sono state effettuate ispezioni, tra l'altro, presso il cantiere di

Ardea (19 gennaio 2023), nei confronti di L'Igiene Urbana Evolution s.r.l. (26 e 27 gennaio 2023), nei confronti di DM Technology s.r.l. (30 maggio 2023) e di Unica s.r.l.s. (30 maggio 2023).

In data 19 gennaio 2023, il Nucleo, unitamente al personale dell'Autorità, si è recato presso il cantiere sito in Ardea, dove ha acquisito a verbale le seguenti dichiarazioni:

“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” (verbale ispettivo 19/1/2023, p. 2);

“all'interno di un locale adiacente al parco automezzi è presente un dispositivo di riconoscimento dei dipendenti basato sulla biometria del volto” (verbale cit., p. 3);

è stato altresì 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. È stato verificato che ai dati di tali ulteriori soggetti non è possibile accedere con le credenziali in possesso della parte” (verbale cit., p. 3).

In data 26 gennaio 2023, nel corso dell'accertamento ispettivo effettuato presso la sede amministrativa di L'Igiene Urbana Evolution s.r.l., quest'ultima ha dichiarato che “la società ha formalizzato nel mese di marzo 2021, con la società Unica srls, l'acquisto dei dispositivi di rilevazione delle presenze, i quali sono stati materialmente installati dalla DM Technology srl in virtù di un pregresso contratto di servizio e di manutenzione” (verbale cit., p. 4).

Il 27 gennaio 2023, sono proseguite le attività ispettive presso la sede amministrativa di L'Igiene Urbana Evolution s.r.l. In tale occasione quest'ultima ha ulteriormente dichiarato che:

“UNICA srls è la società che fornisce attività di consulenza amministrativa, organizzativa e tecnica” (verbale ispettivo 27/1/2023, p. 2);

nel corso dell'accesso al sistema Junior Web, con profilo Admin è “stato visualizzato il prospetto di timbrature del mese di dicembre 2022, comprendente i dipendenti di diversi siti (indicati come CDC, centri di costo). [...] di tutti i centri di costo visualizzati solo 10 fanno riferimento alla società. I restanti CDC fanno riferimento ad altre società, per le quali la DM Technology fornisce assistenza sui dispositivi di rilevazione biometrica” (verbale cit., p. 3);

“gli account per accedere a Junior Web sono forniti e gestiti da DM Technology, che gestisce anche gli account di accesso al dispositivo” (verbale cit., p. 3);

“i dispositivi posti presso i siti di Igiene Urbana Evolution sono collegati con un server posto presso la sede della società [...], per l'invio dei dati relativi alle timbrature. I dispositivi posti presso i siti di altre società si collegano a rispettivi e differenti server. I dati sono poi integrati da DM Technology, per la visualizzazione con il profilo Admin” (verbale cit., p. 4).

Visti i risultati degli accertamenti effettuati in precedenza presso il cantiere di Ardea e presso la sede di L'Igiene Urbana Evolution s.r.l., l'Autorità ha ritenuto necessario effettuare accertamenti ispettivi anche presso la sede legale di DM Technology s.r.l. (di seguito, la Società) al fine di verificare l'eventuale trattamento di dati personali da parte della Società.

Nel corso dell'ispezione, svoltasi in data 30 maggio 2023, la Società ha dichiarato che:

“l'applicativo Junior Web è stato reso disponibile [dal fornitore], in base al contratto sottoscritto con Unica s.r.l.s. [...]. Anche la prima installazione di Junior Web, successiva

all'acquisto della licenza da parte di Unica, è stata effettuata da G. Osti [dal fornitore], da remoto, presso una sede DM" (verbale ispettivo 30 maggio 2023, p. 2);

"delle tre utenze assegnate [dal fornitore], una utenza, utilizzata da DM, aveva profilo Admin, con possibilità di operare completamente sull'applicativo e avere visibilità dei dati delle 3 aziende, una utenza di tipo manager abilitata su uno specifico centro di costo (in genere assegnata al capocantiere) e un profilo di tipo utente semplice, non utilizzato" (verbale cit., p. 3);

"una volta andato a regime l'uso dei dispositivi FD3, la DM ha effettuato assistenza su Junior Web per Unica, Igiene Urbana e DM stessa [...] tramite [l'utenza fornita dal fornitore] era possibile vedere i dati delle timbrature dei centri di costo appartenenti a Unica, Igiene Urbana Evolution e DM" (verbale cit., p. 3);

i 4 dispositivi FD3 "sono posti presso alcuni cantieri DM, non più funzionanti da gennaio 2023 e scollegati dalla rete. I dati sono ancora presenti sui dispositivi" (verbale cit., p. 3);

è stata fornita copia dell'informativa rilasciata ai dipendenti in relazione all'utilizzo degli apparati FD3 (verbale cit., p. 3 e All. 5);

all'interno del registro delle attività di trattamento "aggiornato alla data del 12 marzo 2021 [...] è censito il trattamento effettuato tramite il dispositivo Anviz" (verbale cit., p. 3);

con riguardo alla effettuazione di una valutazione di impatto ai sensi dell'art. 35 del Regolamento la Società ha dichiarato che "è stata effettuata una valutazione sulla base della documentazione fornita dal produttore e dal rivenditore per l'Italia, che assicurava la conformità al GDPR, senza aver formalizzato detta valutazione in un apposito documento" (verbale cit., p. 4).

Alla luce degli esiti degli accertamenti già svolti, è stata disposta l'effettuazione di accertamenti ispettivi anche presso la sede legale di Unica s.r.l.s., svoltisi in data 30 maggio 2023, nel corso dei quali quest'ultima ha dichiarato che:

"la società, nata a gennaio 2020, presta attività di consulenza ai propri clienti [...] a partire da fine 2020 sono iniziati i rapporti con Igiene Urbana Evolution e DM Technology mediante sottoscrizione di apposite convenzioni" (verbale ispettivo 30/5/2023, p. 2 e All. 1 "Convenzione di consulenza/assistenza professionale" con DM Technology, del 20/10/2020 e All. 2 "Convenzione consulenza in materia di lavoro/assistenza professionale" con L' Igiene Urbana Evolution, del 28/12/2020);

le due società sopra menzionate (L' Igiene Urbana Evolution e DM Technology) "hanno rappresentato la necessità di sottoporre ad un maggiore controllo i lavoratori operanti presso alcuni siti di raccolta rifiuti, in particolare il sito di Ardea. Dopo un'analisi di mercato comprensiva anche di una verifica di adeguatezza rispetto alla normativa privacy, la società ha avviato la fornitura, a titolo gratuito, degli apparati FD3, acquisiti a sua volta [dal fornitore], mediante apposito contratto comprensivo anche di 3 licenze di utilizzo del software JuniorWeb. In particolare sono stati forniti 10 apparati a Igiene Urbana e 4 a DM. DM Tech è stato inoltre il soggetto delegato alla gestione e installazione del software Junior Web, in quanto la società DM fornisce attività di consulenza informatica e supporto tecnico ad Unica" (verbale cit., p. 2 e 3).

3. L'avvio del procedimento per l'adozione dei provvedimenti correttivi e le deduzioni della Società.

Il 13 settembre 2023, l'Ufficio 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, 28 e 35 del Regolamento.

Con memorie difensive inviate in data 13 ottobre 2023 (integrate il successivo 26 ottobre), la Società ha dichiarato che:

“Attesa la contiguità della posizione della Scrivente rispetto a quella de L'Igiene Urbana Evolution s.r.l., si ritiene in premessa utile richiamare, per gli aspetti di comune interesse, tutti gli argomenti addotti negli scritti difensivi della predetta società”;

“si fa presente che, con comunicazione mail del 07.06.2023 che si allega alla presente [...], la Società ha indicato i siti presso cui erano installati i dispositivi, con specificazione della data di installazione, del numero dei dipendenti interessati e dell'indirizzo”;

“il modello di informativa fornita agli interessati prevedeva comunque la prestazione del consenso alla rilevazione mediante l'utilizzo dei dati biometrici, con la possibilità in alternativa, per chi non intendesse prestarlo, di adoperare i fogli presenza all'uopo previsti”;

“La Società ha ritenuto, sulla base di un'interpretazione letterale delle previsioni di cui all'art. 9, par. 2, lett. a), del GDPR e dell'evoluzione tecnologica, con la sempre maggiore diffusione dell'uso di dispositivi biometrici in diversi ambiti, che il consenso rappresentasse comunque una delle condizioni alternative di legittimità del trattamento dei dati personali appartenenti a categorie particolari e che potesse essere utilizzato anche in ambito lavorativo”;

“allo stato, non risultano presenti nelle norme di riferimento citate da codesta Autorità, né nel provvedimento ricognitivo di giugno 2019 delle prescrizioni inerenti il trattamento dei particolari in ambito lavorativo (adottato ai sensi delle disposizioni transitorie di cui al d.lgs. 101/2018), previsioni o indicazioni specifiche riguardo all'inutilizzabilità del presupposto del consenso del dipendente in ambito lavorativo, né tanto meno sul divieto assoluto di trattamento di dati biometrici per finalità di rilevazione presenze dei dipendenti”;

“Prima di procedere al trattamento la Società ha [...] effettuato una attenta ricerca di mercato, effettuando una attenta valutazione ed acquisendo la documentazione di conformità al GDPR fornita dai soggetti altamente specializzati a cui si era rivolta. [...] la Società si è focalizzata soprattutto sulle garanzie relative alle misure di sicurezza che offrivano i dispositivi in ordine al trattamento dei dati [...] Sulla base di questa attenta analisi tecnica, è stata altresì valutata la necessità e proporzionalità del trattamento dei dati in relazione alla finalità perseguita (lett. b) dell'art. 35.7 cit.), come attestato dai fornitori che hanno confermato la legittima utilizzabilità dei dispositivi biometrici a fini di rilevazione presenze dei lavoratori nel caso in esame, e tenuto conto che i dati biometrici erano tutelati da misure di sicurezza certificate conformi al GDPR. Si è ritenuto quindi che le misure adottate fossero in grado di mitigare adeguatamente i rischi per i diritti e le libertà degli interessati [...] Non sembra, quindi, si possa parlare nel caso di specie di omessa adozione della DPIA, quanto piuttosto di un vizio relativo alla relativa formalizzazione della stessa in un apposito documento dedicato ad hoc [...]”;

con riferimento alla contestata violazione dell'art. 28 del Regolamento “pur evidenziando come in esito alla ispezione si sia provveduto [...] mediante la formalizzazione delle nomine da parte di committenti per i quali la Società rende i propri servizi [...], si ritiene di evidenziare come la contestazione, ove fondata, sembrerebbe se del caso dover esser mossa ai committenti medesimi, e non alla Scrivente.”;

con riguardo alla valutazione della gravità della violazione si invita l'Autorità a tenere conto, tra l'altro, delle “incertezze e difficoltà interpretative del quadro normativo quanto alla base

giuridica applicabile al trattamento”;

“Con specifico riguardo al tempo di utilizzo dei dispositivi per il riconoscimento facciale presso le 4 unità produttive di DMT dove era installato [...], si evidenzia che, come documentato con la produzione allegata ai presenti scritti, l'utilizzo di tali dispositivi per 3 siti (per un totale di 138 dipendenti ivi operanti) è durato pochi mesi tra, rispettivamente settembre, ottobre e novembre 2022 - date differenziate di loro attivazione - ed il gennaio 2023, data della sua disattivazione da tutte le unità produttive coinvolte, mentre per un sito di DMT in cui operano 19 dipendenti risulta un'attivazione a partire da luglio 2020”;

“la immediata disattivazione da tutte le unità coinvolte dei dispositivi di rilevazione biometrica, rappresenta una doverosa misura di attenuazione [...] delle conseguenze della violazione, oltre alla definizione della procedura per la loro dismissione”.

Nel corso dell'audizione richiesta dalla Società, tenutasi in data 4 dicembre 2023, la stessa ha infine sostenuto, tra l'altro, che:

da parte della Società “c'è stata massima disponibilità nell'ambito dell'attività ispettiva”;

“rispetto alle richieste formulate dai lavoratori nei reclami presentati all'Autorità, a seguito dell'accertamento ispettivo la Società ha immediatamente disposto la sospensione in via cautelativa del trattamento effettuato fino a quel momento tramite il sistema di riconoscimento facciale”;

“il sistema di riconoscimento facciale era stato utilizzato perché, anche erroneamente, era stata interpretata la base giuridica”;

“seppur la Società non abbia adempiuto a tutti gli obblighi imposti dalla normativa di protezione dei dati, ha tenuto conto della sicurezza del dato, adottando le massime misure di sicurezza previste”;

“i lavoratori avevano prestato il consenso al trattamento anche se poi la Società ha scoperto che tale condizione non era sufficiente”;

“Anche in DM Technology s.r.l. vi era, per la rilevazione delle presenze, oltre al riconoscimento facciale, un sistema alternativo basato su un modulo cartaceo”;

“L'Igiene Urbana e DM Technology non hanno provveduto alla cancellazione dei dati in attesa della definizione del procedimento e in vista di ulteriori controlli da parte dell'Autorità. È però già stata prevista una procedura per la cancellazione dei dati raccolti con il sistema di riconoscimento facciale che verrà attivata appena concluso il procedimento dinanzi all'Autorità”.

4. L'esito dell'istruttoria e del procedimento per l'adozione dei provvedimenti correttivi e sanzionatori.

4.1 Violazioni della Società in qualità di titolare del trattamento. Violazione dell'art. 5, par. 1, lett. a) e 9 del Regolamento in relazione ai trattamenti di dati dei propri dipendenti.

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 dipendenti, 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, presso alcuni cantieri, attraverso quattro dispositivi biometrici (v. verbale 30/5/2023, p. 3), disattivati dal mese di gennaio 2023 e allo stato "scollegati dalla rete".

Come evidenziato dalla Società nelle proprie memorie difensive, in data 7 giugno 2023 quest'ultima ha trasmesso all'Autorità, a scioglimento della riserva effettuata in occasione dell'accertamento ispettivo, un prospetto dal quale si evince che i trattamenti di dati biometrici hanno riguardato un totale di 157 dipendenti (in forza presso le sedi di Scafati, Quarto, Orta di Atella e San Marzano).

Per quanto riguarda la durata del trattamento, relativamente a 19 dipendenti (presso la sede di Scafati), questo è iniziato il 1° luglio 2020 e cessato il 26 gennaio 2023. I trattamenti relativi agli altri 138 dipendenti sono iniziati il 29 settembre (sede di Orta di Atella, 59 dipendenti), 1° ottobre (sede di Quarto, 63 dipendenti) e 11 novembre 2022 (sede di San Marzano, 16 dipendenti) e cessati tra il 23 e il 26 gennaio 2023, dopo l'avvio delle attività ispettive da parte dell'Autorità.

Il numero di dipendenti interessati dal trattamento di dati biometrici è dunque significativo.

Preliminarmente 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 l'ordinamento vigente non consente il trattamento di dati biometrici dei dipendenti per finalità di rilevazione della presenza in servizio. Ciò è stato ribadito dal Garante con i provvedimenti n. 369 del 10 novembre 2022 (doc. web n. 9832838) e n. 16 del 14 gennaio 2021 (doc. web n. 9542071).

L'utilizzo del dato biometrico nel contesto dell'ordinaria gestione del rapporto di lavoro (quale è l'attività di rilevazione delle presenze) non è pertanto conforme ai principi di minimizzazione e proporzionalità del trattamento (art. 5, par. 1, lett. c) del Regolamento).

Inoltre, si rileva che 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"; si veda inoltre: 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).

Né, quale condizione di liceità del trattamento dei dati biometrici, può soccorrere la prestazione del consenso da parte del dipendente, come prevista nel modello di informativa fornita agli interessati ai sensi dell'art. 13 del Regolamento, datata 12/3/2021 e acquisita in atti (v. verbale ispettivo 30/5/2023, All. 5).

All'interno della predetta informativa che contempla, tra l'altro, il trattamento di dati biometrici per finalità di rilevazione della presenza e "alternativamente [...] la registrazione attraverso l'attestazione sui fogli presenza", è presente - in fine - la possibilità di prestare o negare il consenso per "le attività sopra descritte per le quali il consenso rappresenta la base giuridica del trattamento", con la specificazione che "qualora l'interessato non intenda prestare il consenso alla rilevazione della presenza mediante l'utilizzo dei dati biometrici, potrà adoperare i fogli presenza all'uopo previsti".

Come già rilevato sopra, in relazione ai trattamenti di dati particolari effettuati nell'ambito del rapporto di lavoro, il Regolamento prevede la sussistenza del requisito di cui all'art. 9, par. 2, lett. b), e non già la prestazione del consenso posto che tale condizione di liceità, come costantemente affermato dal Garante, 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 (v., tra gli altri, provv. 10/11/2022, n. 369, doc. web n.

9832838).

In base ai suesposti motivi 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.

4.2 Violazione dell'art. 35 del Regolamento.

In base all'art. 35 del Regolamento, 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 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 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 (v. cap. III, B, n. 4), il trattamento effettuato nei confronti di interessati "vulnerabili" (ad es. in quanto parti di un rapporto di lavoro; v. cap. III, B, n. 7) nonché i trattamenti che realizzano un "uso innovativo o [l']applicazione di nuove soluzioni tecnologiche od organizzative" (v. cap. III, B, n. 8).

Ulteriori indicazioni 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.

Pur avendo adottato un sistema di autenticazione biometrica per finalità di rilevazione delle presenze dei propri dipendenti, non è emerso che la Società abbia provveduto ad effettuare una valutazione di impatto prima dell'inizio dei trattamenti stessi, posto che, secondo quanto dichiarato, una valutazione sarebbe stata effettuata ma "senza aver[la] formalizzat[a] [...] in un apposito documento".

Infatti, conformemente al principio di responsabilizzazione del titolare (v. art. 5, par. 2 del Regolamento), la valutazione di impatto deve essere adeguatamente formalizzata in un documento che, tra l'altro, possa essere esaminato dall'Autorità di controllo, tenuto anche conto che l'art. 35 del Regolamento individua il contenuto necessario minimo della valutazione stessa (par. 7).

La Società pertanto non ha osservato quanto disposto dall'art. 35 del Regolamento.

4.3 Violazioni della Società in qualità di responsabile del trattamento. Violazione dell'art. 28 del Regolamento.

È altresì emerso che la Società, attraverso l'accesso con profilo Admin all'applicativo Junior Web, ha avuto accesso ai dati relativi alle timbrature dei dipendenti di Unica s.r.l.s. e L'Igiene Urbana Evolution s.r.l. (v. verbale ispettivo 30/5/2023, p. 3), Airone società consortile a r.l. e Blu Work s.r.l. (v. verbale ispettivo 27/1/2023 nei confronti di L'Igiene Urbana Evolution s.r.l., p. 3 e 4).

Posto che le scelte relative a finalità e mezzi del trattamento stesso sono state definite da L'Igiene Urbana Evolution s.r.l., Airone società consortile a r.l., Blu Work s.r.l. e Unica s.r.l.s. in qualità di titolari/datori di lavoro, la Società ha effettuato un trattamento, per conto dei titolari del trattamento, senza che ciò fosse stato preventivamente disciplinato da un contratto o altro atto giuridico,

secondo quanto previsto dall'art. 28 del Regolamento e in assenza di specifiche istruzioni predisposte da questi ultimi.

Non risulta infatti che l'Igiene Urbana Evolution s.r.l., Airone società consortile a r.l., Blu Work s.r.l. e Unica s.r.l.s. abbiano, in relazione ai trattamenti effettuati, provveduto a designare la Società quale responsabile del trattamento, come previsto dall'art. 28 del Regolamento.

D'altra parte, neppure la convenzione stipulata tra DM Technology e L'Igiene Urbana, acquisita in atti, contiene gli elementi espressamente indicati dall'art. 28, par. 3 del Regolamento (v. Convenzione per manutenzione del 28/10/2020, All. 2, verbale ispettivo 27/1/2023 nei confronti di L'Igiene Urbana Evolution s.r.l.).

Il titolare del trattamento nell'ambito della predisposizione delle misure tecniche e organizzative che soddisfino i requisiti stabiliti dal Regolamento, anche sotto il profilo della sicurezza (artt. 24 e 32 del Regolamento), può avvalersi di un responsabile per lo svolgimento di alcune attività di trattamento, cui impartisce specifiche istruzioni (cfr. considerando 81 del Regolamento).

In tal caso il titolare "ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto [le predette misure] adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti degli interessati" (art. 28, par. 1, del Regolamento).

Ai sensi dell'art. 28 del Regolamento, il titolare può quindi affidare un trattamento anche a soggetti esterni, disciplinandone il rapporto con un contratto o un altro atto giuridico e impartendo le istruzioni in merito alle caratteristiche principali del trattamento.

Il responsabile del trattamento è, pertanto, legittimato a trattare i dati degli interessati "soltanto su istruzione documentata del titolare" (art. 28, par. 3, lett. a), del Regolamento), ciò anche al fine di impedire l'effettuazione di trattamenti di dati in assenza di un idoneo presupposto di liceità (v. la definizione di "terzo" ex art. 4, n. 10 del Regolamento).

Né può essere accolta l'obiezione formulata dalla Società nelle memorie difensive secondo la quale "laddove il titolare a tale nomina non abbia provveduto, è allo stesso, e non al potenziale responsabile, che [...] si sarebbe dovuto e si sarebbe potuto eventualmente addebitare l'inadempimento" e mai l'Autorità si sarebbe pronunciata in tal senso.

In proposito si rappresenta che, diversamente da quanto sostenuto dalla Società, il Garante ha più volte stabilito con proprie decisioni che la violazione dell'art. 28 del Regolamento deve essere imputata anche al responsabile, in quanto, in assenza del contratto o di altro atto giuridico, le attività di trattamento di dati da lui effettuati avverrebbero in assenza di idonea base giuridica (v., tra gli altri, provv. 15/12/2022, n. 427, doc. web n. 9856694; provv. 11/2/2021, n. 49, doc. web n. 9562852; provv. 17/9/2020, n. 160 e 161, doc. web nn. 9461168 e 9461321). In senso conforme si è anche espressa la Corte di Cassazione (v. ord. 35256/2023, spec. punto 2.4.).

Per i suesposti motivi la Società ha violato l'art. 28 del Regolamento.

5. Conclusioni: dichiarazione di illiceità del trattamento. Provvedimenti correttivi ex art. 58, par. 2, Regolamento.

Per i suesposti motivi, l'Autorità ritiene che 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, 28 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 (v. Considerando 148 del Regolamento).

L'Autorità prende 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 “una procedura per la cancellazione dei dati raccolti con il sistema di riconoscimento facciale che verrà attivata appena concluso il procedimento dinanzi all'Autorità” (v. verbale audizione 4/12/2023).

Pertanto, visti i poteri correttivi attribuiti dall'art. 58, par. 2 del Regolamento, si dispone una sanzione amministrativa pecuniaria ai sensi dell'art. 83 del Regolamento, commisurata alle circostanze del caso concreto (art. 58, par. 2, lett. i) Regolamento).

6. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i), e 83 del Regolamento; art. 166, comma 7, del Codice).

All'esito del procedimento risulta che DM Technology s.r.l. ha violato gli artt. 5, par. 1, lett. a), 9, 28 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) del Regolamento, mediante adozione di un'ordinanza ingiunzione (art. 18, l. 24.11.1981, n. 689).

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, nel caso di specie, sono state considerate 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 abbreviato d'esercizio per l'anno 2022. Da ultimo si tiene conto dell'entità delle sanzioni irrogate in casi analoghi.

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene, nel caso di specie, di applicare nei confronti di DM Technology s.r.l. la sanzione amministrativa del pagamento di una somma pari ad euro 20.000 (ventimila).

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.

TUTTO CIÒ PREMESSO, IL GARANTE

rileva l'illiceità del trattamento effettuato da DM Technology s.r.l., in persona del legale rappresentante, con sede legale in Via Leonardo da Vinci, 5, Scafati (SA), C.F. 05880000657, ai sensi dell'art. 143 del Codice, per la violazione degli artt. 5, par. 1, lett. a), 9, 28 e 32 del Regolamento;

ORDINA

ai sensi dell'art. 58, par. 2, lett. i) del Regolamento a DM Technology s.r.l., di pagare la somma di euro 20.000 (ventimila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento;

INGIUNGE

quindi alla medesima Società di pagare la predetta somma di euro 20.000 (ventimila), secondo le modalità indicate in allegato, entro 30 giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dell'art. 27 della legge n. 689/1981. Si ricorda che resta salva la facoltà per il trasgressore di definire la controversia mediante il pagamento – sempre secondo le modalità indicate in allegato - di un importo pari alla metà della sanzione irrogata, entro il termine di cui all'art. 10, comma 3, del d. lgs. n. 150 dell'1.9.2011 previsto per la proposizione del ricorso come sotto indicato (art. 166, comma 8, del Codice);

DISPONE

la pubblicazione del presente provvedimento sul sito web del Garante ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/20129, e ritiene che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

Richiede a DM Technology s.r.l. di comunicare quali iniziative siano state intraprese al fine di cancellare i dati biometrici oggetto di conservazione sui dispositivi, e di fornire comunque riscontro adeguatamente documentato ai sensi dell'art. 157 del Codice, entro il termine di 90 giorni dalla data di notifica del presente provvedimento; l'eventuale mancato riscontro può

comportare l'applicazione della sanzione amministrativa prevista dall'art. 83, par. 5, lett. e) del Regolamento.

Ai sensi dell'art. 78 del Regolamento, nonché degli articoli 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo individuato nel medesimo art. 10, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 22 febbraio 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Mattei