Provvedimento del 14 settembre 2023 [9940565]

[doc. web n. 9940565]

Provvedimento del 14 settembre 2023

Registro dei provvedimenti
n. 404 del 14 settembre 2023

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti e il dott. Claudio Filippi, vice segretario generale;

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

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

VISTO il reclamo presentato dal sig. XX in data 20/09/2021, ai sensi dell'art. 77 del Regolamento, con cui è stata lamentata una violazione della disciplina in materia di protezione dei dati personali da parte di Nimbus s.r.l.;

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 la prof.ssa Ginevra Cerrina Feroni;

PREMESSO

1. L'avvio del procedimento.

Con il reclamo datato 20/09/2021, il sig. XX ha rappresentato che, in data 06/11/2019, è stato assunto dalla società Nimbus s.r.l. con contratto di lavoro a tempo determinato e di aver svolto la sua attività lavorativa presso la sede di viale Coni Zugna n. 71, in Milano. Con il reclamo, è stato lamentato che, presso la sede di lavoro, era presente un sistema di rilevazione delle presenze basato sulla lettura delle impronte digitali introdotto senza che fosse stata resa un'informativa o richiesto un consenso al riguardo.

Con la nota datata 27/10/2021 (prot. n. 53982), l'Ufficio formulava nei confronti della Società una richiesta di informazioni, ai sensi dell'art. 157 del d.lgs. 196/2003 (recante il Codice in materia di protezione dei dati personali, di seguito "Codice"), volta a conoscere le caratteristiche principali del sistema biometrico, nonché i presupposti di legittimità del trattamento e le specifiche finalità che

hanno reso necessario l'utilizzo del sistema di rilevamento biometrico.

La Società forniva riscontro, con la nota del 19/11/2021, con la quale dichiarava che:

- il sistema di rilevazione delle presenze tramite impronte digitali è stato attivato in data 1° febbraio 2019;

- l'azienda XX ha provveduto all'installazione del sistema in argomento, "assicurando che le modalità di utilizzo del dispositivo stesso erano pienamente rispettose della vigente normativa in materia di protezione dei dati personali";

- l'Ispettorato del lavoro territorialmente competente, con una e-mail del 10/11/2021, in riscontro a una precisa richiesta della Società, ha confermato che l'installazione del sistema di rilevazione delle presenze, basato sul riconoscimento biometrico, non richiede l'autorizzazione di cui all'art. 4 della legge 300/1970.

Quanto alle caratteristiche tecniche del sistema biometrico in uso, la Società ha allegato la relazione tecnica predisposta dalla società installatrice da cui risulta che:

- "il dispositivo installato dall'Azienda (…) è una timbratrice marcatempo rilevatore delle presenze dotata di lettore biometrico (impronte digitali). Utilizzando il dispositivo, il personale può certificare i propri ingressi/uscite dal posto di lavoro attraverso le modalità previste, ovvero l'impronta digitale o, in alternativa, un ID univoco (numerico) associato ad ogni lavoratore e la relativa password assegnata";

- "Il dispositivo risulta conforme alle normative in materia di tutela della privacy, in quanto le impronte digitali personali sono raccolte e memorizzate esclusivamente nella memoria interna del dispositivo stesso e sono rese di fatto indecifrabili/inutilizzabili in qualsiasi altro ambito, grazie al particolare algoritmo con la quale sono criptate. Inoltre le stesse sono di fatto non leggibili/esportabili per usi diversi, data la non accessibilità della memoria interna del dispositivo";

- "Le caratteristiche individuali del polpastrello sono vettorializzate in punti univoci e convertite dal terminale in un codice numerico complesso, utilizzando uno speciale algoritmo. Il numero di dipendente corrispondente pertanto è collegato a tale valore".

Con successiva nota del 29/01/2022, la Società in riscontro a una richiesta di integrazioni dell'Ufficio precisava che:

- ai propri dipendenti è stata resa un'informativa, ai sensi dell'art. 13 del Regolamento, in cui si legge che "Non vengono invece trattati dati genetici o biometrici che la riguardano"; e ciò in quanto il dispositivo iAccess non memorizza in nessun caso le immagini dell'impronta digitale, elaborando solo un modello di riferimento anonimo e virtuale";

- la Società opera in due sedi e in entrambe sono presenti i sistemi di rilevamento biometrico della presenza, coinvolgendo 13 dipendenti;

- con riferimento ai presupposti di legittimità del trattamento, questi "non sono minimamente in discussione, in quanto, come già detto, non vi è memorizzazione di dati biometrici e quindi non vi è neppure trattamento degli stessi";

- "quanto alle finalità dell'installazione del dispositivo iAccess, lo stesso è stato progettato, realizzato e utilizzato per la rilevazione delle presenze in funzione della gestione del rapporto di lavoro";

- “La procedura di acquisizione (enrolment) e la relativa iscrizione nel sistema degli utenti, nell’impianto in oggetto, (…) avviene attraverso il terminale stesso che, nella fase di acquisizione viene utilizzato come un lettore al fine di rilevare il campione associandolo ad un ID precedentemente attribuito all’utente a mezzo del software di interfaccia/gestione unitamente al nome e cognome. Si ribadisce che gli utenti possono gestire attraverso quell’ID accesso e marcatura a prescindere dall’utilizzo e della rilevazione del campione biometrico che in nessun caso è stato imposto agli stessi. Successivamente il campione stesso è memorizzato, criptato da apposito algoritmo sviluppato dal produttore e reso di fatto indecifrabile/inutilizzabile in qualsiasi altro ambito che non sia il riconoscimento e la marcatura della presenza, attraverso il descritto dispositivo. (…) Inoltre il dispositivo stesso è interfacciato a mezzo connessione Lan ad una singola postazione dedicata, esclusa dalla rete aziendale, protetta da password di accesso, disponibile agli incaricati al solo fine di scaricare la reportistica di accessi/presenze per le necessità di elaborazione aziendale”;

- la modalità di confronto del modello biometrico al momento della rilevazione è di uno a uno;

- “Il dato grezzo viene cancellato al termine della procedura di accesso/timbratura, il campione (presente esclusivamente e con le caratteristiche sopra esposte all’interno del dispositivo, ovvero sotto forma di algoritmo indecifrabile/inutilizzabile esternamente) entro 24h dalla cessazione del rapporto, attraverso la rimozione dell’ID utente e del relativo dato acquisito. Si ribadisce che tutti i dati sono memorizzati esclusivamente nel dispositivo; lo stesso, alla timbratura, identificato l’utente, trasmette alla postazione dedicata ed al relativo software gestionale l’ID utente e gli orari di ingresso e uscita, senza alcuna altra informazione”.

Sulla base delle dichiarazioni rese dalla Società, l’Ufficio provvedeva a notificare alla società l’atto di avvio del procedimento sanzionatorio, ai sensi dell’art. 166, comma 5, del Codice in relazione alla violazione degli artt. 5, par. 1, lett. a), 6, 9, par. 2, lett. b), e 13 del Regolamento (nota del 14/04/2022, prot. n. 20869).

La Società inviava, in data 11/05/2022, propri scritti difensivi, ai sensi dell’art. 18 della legge n. 689/1981, con cui sottolineava la propria buona fede nel trattamento in esame, avendo ricevuto precise garanzie da parte della società installatrice del sistema di rilevamento biometrico circa la correttezza del trattamento posto in essere.

Veniva, inoltre, rappresentato che, in data 30/04/2022, si era provveduto alla “rimozione dei dispositivi di rilevamento delle presenze dei dipendenti tramite impronte digitali, sostituendo in entrambe le unità locali gli apparati esistenti con sistemi di rilevazione a mezzo “badge”, che non rilevano nel modo più assoluto dati biometrici; è stato quindi rimosso il software preesistente e sono stati cancellati tutti i dati dei dipendenti già memorizzati”.

In data 01/02/2023, si è tenuta l’audizione della Società, ai sensi dell’art. 18 della legge n. 689/1981, nel corso della quale la Società ha ribadito la mancanza di colpevolezza nelle operazioni di trattamento oggetto di contestazione.

2. L’esito dell’istruttoria.

All’esito dell’esame della documentazione prodotta e delle dichiarazioni rese dalla parte nel corso del procedimento, premesso 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, è emerso che la società, in qualità di titolare del trattamento, ha effettuato un trattamento di dati personali, riferito ai propri dipendenti, che non sono conformi alla disciplina in materia di protezione dei dati personali.

2.1. Il trattamento di dati biometrici effettuato dalla Società. Violazione dell'art. 9, par. 2, lett. b), del Regolamento.

Nel merito, è emerso che la Società ha effettuato, a partire dal mese di febbraio 2019, un trattamento di dati personali, riferito a 13 dipendenti, per mezzo di un sistema di rilevamento biometrico, installato presso le due unità lavorative e finalizzato alla registrazione delle presenze in servizio.

In particolare, tale sistema era basato sulla rilevazione dell'impronta digitale le cui caratteristiche principali venivano convertite in un codice numerico, associato al dipendente.

Tale sistema, è stato, nel corso del procedimento, rimosso e sostituito con un sistema di rilevazione basato su badge (memorie difensive dell'11/05/2022).

I trattamenti di dati personali effettuati dalla Società hanno, pertanto, riguardato i dati biometrici dei dipendenti, alla luce dei numerosi interventi dell'Autorità che con propri provvedimenti ha chiarito che tale tipologia di trattamenti si configura sia nella fase di registrazione (c.d. enrollment, consistente nella acquisizione delle caratteristiche biometriche – nella specie impronte digitali - dell'interessato (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).

Sul punto, occorre richiamare la definizione di dati biometrici fornita dal Regolamento, secondo cui sono tali i "dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici" (art. 4, n. 14, del Regolamento).

In base alla disciplina in materia di protezione dei dati personali, inoltre, 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 medesimo 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. pure, art. 88, par. 1 e cons. 51-53 del Regolamento).

Come è stato più volte chiarito dall'Autorità, 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 (in quanto implicano un trattamento "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]"), 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) (v. da ultimo provvedimento dell'Autorità n. 369 del 10/11/2022, doc web n. 9832838).
Pertanto, affinché un trattamento avente a oggetto dati biometrici possa essere lecitamente realizzato è necessario che lo stesso trovi il proprio fondamento in una disposizione normativa che abbia le caratteristiche richieste dalla disciplina di protezione dei dati, anche in termini di proporzionalità dell'intervento regolatorio rispetto alle finalità che si intendono perseguire.

Allo stato non sussiste un'idonea base giuridica che possa soddisfare i requisiti richiesti dal Regolamento e dal Codice per legittimare i titolari del trattamento a porre in essere il trattamento dei dati biometrici per finalità di rilevazione delle presenze dei dipendenti ai sensi dell'art. 9, par. 2, lett. b) del Regolamento.

Alla luce di quanto sopra, si rileva che il trattamento di dati biometrici posto in essere dalla Società è stato effettuato in assenza di un'idonea base giuridica, in violazione dell'art. 9, par. 2, lett. b) del Regolamento.

2.2. Violazione degli artt. 5, par. 1, lett. a) e 13 del Regolamento.

In base alla disposizione di cui all'art. 5, par. 1, lett. a), del Regolamento, il titolare del trattamento deve trattare i dati "in modo lecito, corretto e trasparente", laddove con particolare riferimento al contesto del rapporto di lavoro l'obbligo di informare il dipendente è altresì espressione del dovere di correttezza.

All'esito dell'istruttoria è emerso che nell'informativa predisposta dalla Società non vi fosse alcun riferimento al trattamento dei dati biometrici effettuato per la rilevazione delle presenze, né fosse indicata la possibilità di utilizzare, in alternativa al sistema biometrico, il sistema tradizionale basato sul badge (diversamente da quanto dichiarato dalla società fornitrice nella relazione tecnica allegata alla nota del 19/11/2021).

Tale condotta si pone in contrasto con quanto prescritto dall'art. 13 del Regolamento, in base al quale il titolare del trattamento deve fornire agli interessati un'informativa che presenti le caratteristiche principali del trattamento che intende effettuare, indicando tra l'altro le finalità e le modalità del trattamento, la base giuridica e i tempi di conservazione dei dati trattati.
Per tali motivi, si rileva che la società ha effettuato un trattamento di dati biometrici dei dipendenti in violazione degli artt. 5, par. 1, lett. a) e 13 del Regolamento, dalla data di installazione e messa in funzione dei dispositivi, come risulta in atti, fino alla data della cessazione avvenuta in data 30/04/2022.

3. 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 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 biometrici posto in essere dalla società risulta illecito, in quanto, per motivi su esposti, in violazione degli artt. 5, par. 1, lett. a), 9, par. 2, lett. b) e 13 del Regolamento.

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

4. 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).

Il Garante, ai sensi dell'art. 58, par. 2, lett. i) del Regolamento e dell'art. 166 del Codice, ha il potere di infliggere una sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento, mediante l'adozione di una ordinanza ingiunzione (art. 18. legge 24 novembre 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 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:

- in relazione alla natura, gravità e durata della violazione, sono state prese in considerazione la circostanza che il trattamento ha riguardato categorie particolari di dati e che si è protratto per un periodo di circa tre anni;

- in relazione al carattere doloso o colposo della violazione e al grado di responsabilità del titolare sono state prese in considerazione la condotta e il grado di responsabilità della società connesse all'inosservanza dei principi generali del trattamento;

- l'assenza di precedenti specifici a carico della società relativi a violazioni della disciplina in materia di protezione dei dati personali;

- la cooperazione fornita nel corso dell'istruttoria e, in particolare, l'essersi prontamente conformata alle indicazioni dell'Autorità.

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, nonché del particolare contesto economico legato all'emergenza sanitaria. 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 a Nimbus s.r.l., la sanzione amministrativa del pagamento di una somma pari ad euro 5.000,00 (cinquemila).

In tale quadro si ritiene, altresì, in considerazione della tipologia delle violazioni accertate che hanno riguardato i principi generali 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 Nimbus s.r.l., in persona del legale rappresentante pro tempore, con sede legale in Milano, Via Pisanello n. 21, C.F. 10508630968, ai sensi dell'art. 143 del Codice, per la violazione degli artt. artt. 5, par. 1, lett. a), 9, 13, del Regolamento;

ORDINA

ai sensi dell'art. 58, par. 2, lett. i) del Regolamento a Nimbus s.r.l. di pagare la somma di euro 5.000,00 (cinquemila) 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 5.000,00 (cinquemila), 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.

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, 14 settembre 2023

LA VICEPRESIDENTE
Cerrina Feroni

IL RELATORE
Cerrina Feroni

IL VICE SEGRETARIO GENERALE
Filippi