Provvedimento del 27 marzo 2025 [10138981]

VEDI ANCHE Newsletter del 25 giugno 2025

[doc. web n. 10138981]

Provvedimento del 27 marzo 2025

Registro dei provvedimenti
n. 167 del 27 marzo 2025

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, 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, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, "Regolamento generale sulla protezione dei dati" (di seguito, "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (di seguito "Codice");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione n. 98 del 4 aprile 2019, pubblicato in G.U. n. 106 dell'8 maggio 2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, doc. web n. 1098801;

Relatore l'avv. Guido Scorza;

PREMESSO

1. Introduzione.

Con reclamo presentato ai sensi dell'art. 77 del Regolamento, i Sig.ri XX, XX e XX hanno lamentato, per il tramite del proprio difensore, una presunta violazione della disciplina in materia di

protezione dei dati personali con riguardo all'impiego, presso le sedi dell'Istituto di Istruzione Superiore "P. Galluppi" Tropea, di un sistema di rilevazione delle presenze del personale dipendente amministrativo che, richiedendo l'utilizzo delle impronte digitali dei lavoratori, implicherebbe il trattamento dei relativi dati biometrici al fine di identificarli in modo univoco.

2. L'attività istruttoria.

Al riguardo, nell'ambito dell'istruttoria, con nota del XX, l'Istituto ha dichiarato, in particolare, che:

> "nelle diverse sedi dell'IIS di Tropea il personale ATA attesta la propria presenza in servizio per mezzo di rilevatore con badge acquisito nell'anno scolastico XX […] Nel corso del tempo, tuttavia, [… l'Istituto] ha rilevato situazioni che hanno generato il dubbio sul corretto utilizzo del badge e sulla effettiva presenza in servizio di titolari del badge, oltre ad episodi di manomissioni, danneggiamenti e atti vandalici. Per fare fronte alle azioni suddette e accertarsi della effettiva presenza in servizio dei dipendenti nelle ore previste, la Dirigenza della Scuola ha proposto al personale, a sua esclusiva tutela, l'integrazione del sistema di rilevazione con l'utilizzo dell'impronta digitale in abbinamento al badge, accolto con favore dallo stesso";
>
> "il sistema adottato è stato scelto sulla base della garanzia in ordine alla correttezza del trattamento dati ed alla conformità al GDPR rilasciate dall'azienda fornitrice";
>
> "non si è pensato di dover informare e coinvolgere il DPO, ritenendo sufficienti le indicazioni tecniche e le garanzie fornite dall'azienda oltre al consenso prestato dal personale ATA coinvolto ed anzi alla sollecitazione, da parte dello stesso, circa l'adozione di tale sistema a garanzia di tutti";
>
> "al personale coinvolto, per consentire di esprimere un consenso libero, è stata garantita la possibilità di usare alternativamente il sistema di rilevazione delle presenze con badge senza associazione dell'impronta. […] Tranne i due Signori [… tra i reclamanti], tutto il personale ATA (34 unità), in servizio presso l'Istituto d'Istruzione Superiore di Tropea, ha prestato il consenso all'integrazione del sistema di rilevazione delle presenze […] Agli atti della scuola sono conservati i consensi sottoscritti dal personale ATA interessato";
>
> "a seguito della ricezione del reclamo [ossia in data XX, giorno in cui l'Autorità ha trasmesso all'Istituto una richiesta di informazioni ai sensi dell'art. 157 Codice], [… l'Istituto] ha nell'immediatezza sospeso la rilevazione delle presenze con badge abbinato all'impronta digitale. Ad oggi, nonostante le richieste di tutto il personale ATA (tranne le due unità che hanno presentato reclamo) di riattivazione del sistema badge con impronta, sollevate e sollecitate dallo stesso durante le riunioni di avvio anno XX, con la disponibilità di tutto il personale suddetto a prestare richiesta scritta e ulteriore consenso alla riattivazione del sistema, la rilevazione delle presenze in servizio è attestata con il SOLO uso del badge SENZA impronta".

Quanto, più nello specifico, al funzionamento del sistema di rilevazione delle presenze precedentemente in uso presso l'Istituto, dalla documentazione tecnica trasmessa in allegato alla predetta nota del XX si evince, in particolare, che:

> "il funzionamento del lettore di impronte digitali, quale strumento di verifica biometrica comprende 2 fasi principali: A. Registrazione (enrolment): le caratteristiche dell'impronta digitale sono acquisite tramite il lettore del terminale, digitalizzate, elaborate e compresse mediante un algoritmo matematica irreversibile (da non confondersi con il processo di criptografia o crittografia) fino ad ottenerne un modello matematico (template) che, associato al codice identificativo della persona, diviene la base dei successivi confronti o verifiche; B.

Verifica (matching): le caratteristiche dell'impronta digitale sono acquisite, digitalizzate, elaborate e compresse in modo identico a quello della fase di registrazione fino ad ottenere un analogo modello matematico. Il confronto tra il modello (template) archiviato relativo al codice di riferimento ed il risultato della lettura determina, in base allo scostamento, il risultato della verifica";

"nel [predetto] modello […] vengono memorizzati solo dei numeri di riferimento […] e non la caratteristica biometrica vera e propria. Questo rende impossibile risalire dal template all'impronta stessa, rendendo così sicura, in materia di privacy, l'identità dei soggetti registrati";

"il [predetto] template può essere memorizzato direttamente nella memoria del lettore oppure può essere memorizzato su un badge in dotazione all'utente, in entrambi i casi sono archiviati solo i seguenti dati: codice utente; è un puro codice di riferimento, assimilabile al numero di matricola; modello (template) è un puro numero, assimilabile al codice presente in una banda magnetica di un badge […;] elenco eventi: data/ora, codice utente, indirizzo del terminale ed eventuale codice causale (giustificativo) sono gli unici risultati memorizzati dopo le verifiche operate dal lettore biometrico, dati equivalenti ai dati "classici" di un terminale di gestione presenze";

"nel lettore biometrico del terminale […] non sono quindi presenti: dati anagrafici dell'utente; immagine dell'impronta digitale dell'utente; dati fisici diretti o deducibili dell'impronta digitale".

Con nota del XX, l'Ufficio, sulla base degli elementi acquisiti, dalle verifiche compiute e dei fatti emersi a seguito dell'attività istruttoria, ha notificato all'Istituto, ai sensi dell'art. 166, comma 5, del Codice, l'avvio del procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento, per aver trattato i dati personali biometrici dei dipendenti amministrativi, tecnici e ausiliari (A.T.A.) al fine di identificarli in modo univoco per rilevarne la presenza in servizio, in maniera non conforme al principio di "liceità, correttezza e trasparenza" nonché in assenza di un idoneo presupposto normativo, in violazione degli artt. 5, par. 1, lett. a), 6 e 9 del Regolamento.

Con la medesima nota, il predetto titolare è stato invitato a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentito dall'Autorità (art. 166, commi 6 e 7, del Codice, nonché art. 18, comma 1, della l. 24 novembre 1981, n. 689).

Con nota del XX, l'Istituto, che non ha richiesto di essere audito, ha presentato una memoria difensiva, dichiarando, in particolare, che:

- "il sistema di rilevazione delle presenze tramite badge abbinato all'impronta digitale, è stato avviato [… dall'Istituto] nel XX"

- "contestualmente [alla sospensione dell'impiego del predetto sistema nel XX], sono state effettuate le operazioni di cancellazione di tutti i dati biometrici acquisiti dal sistema e impostato lo stesso per il funzionamento con il solo badge senza associazione dell'impronta".

- "ad oggi […] la rilevazione delle presenze in servizio è attestata con il solo uso del badge senza impronta".

3. Il quadro normativo in materia di protezione dei dati personali.

Con riferimento alla questione prospettata nel reclamo si evidenzia, in via preliminare, che i dati biometrici sono definiti dal Regolamento come "i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati

dattiloscopici" (art. 4, punto 14), del Regolamento) e, laddove intesi a identificare in modo univoco una persona fisica, sono ricompresi tra le categorie "particolari" di dati personali (art. 9 del Regolamento) in ragione della loro delicatezza, derivante dalla stretta e stabile relazione con l'individuo e la sua identità.

Il trattamento di dati biometrici, di regola vietato per effetto del disposto di cui all'art. 9, par. 1, del Regolamento, è consentito esclusivamente al ricorrere di una delle condizioni indicate dell'art. 9, par. 2 del Regolamento e, in ambito lavorativo, solo quando 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).

Il quadro normativo vigente prevede inoltre che il trattamento di dati biometrici, per poter essere lecitamente posto in essere, avvenga nel rispetto di "ulteriori condizioni, comprese limitazioni" (cfr. art. 9, par. 4, del Regolamento); a tale disposizione è stata data attuazione, nell'ordinamento nazionale, con l'art. 2-septies (Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute) del Codice (come modificato dal decreto legislativo 10 agosto 2018 n. 101 di adeguamento della normativa nazionale alle disposizioni del Regolamento). La norma prevede che è lecito il trattamento di tali categorie di dati al ricorrere di una delle condizioni di cui all'art. 9, par. 2, del Regolamento "ed in conformità alle misure di garanzia disposte dal Garante", in relazione a ciascuna categoria dei dati.

Il datore di lavoro, titolare del trattamento, è, in ogni caso, tenuto a rispettare i principi di protezione dei dati personali, tra cui in particolare quelli di "liceità, correttezza e trasparenza", "minimizzazione" e protezione dei dati "fin dalla progettazione" e "per impostazione predefinita" (artt. 5 e 25 del Regolamento).

4. Esito dell'attività istruttoria.

Dall'accertamento compiuto sulla base degli elementi acquisiti e dei fatti emersi all'esito dell'attività istruttoria, nonché delle successive valutazioni dell'Autorità, risulta accertato che, a partire dal XX e sino alla data del XX, l'Istituto ha fatto uso, presso le proprie sedi, di un sistema di rilevazione delle presenze del personale A.T.A. che richiedeva l'utilizzo delle impronte digitali dei lavoratori che avessero rilasciato il proprio consenso, con ciò dando luogo ad un trattamento dei relativi dati biometrici inteso ad identificare in modo univoco i singoli dipendenti al fine di rilevarne la presenza in servizio nonché nell'ottica di prevenire "episodi di manomissioni, danneggiamenti e atti vandalici" (cfr. nota del XX).

In particolare, è stato accertato che il predetto sistema, elaborando le caratteristiche dell'impronta digitale acquisita, permette di creare un modello matematico che, venendo associato al codice identificativo del singolo interessato, costituisce il termine di raffronto delle successive verifiche all'atto della timbratura dei dipendenti.

Ancorché lo stesso non mantenga traccia dei dati anagrafici dei dipendenti, dell'immagine o di "dati fisici diretti o deducibili" delle relative impronte digitali e, per altro verso, "la "ricostruzione dell'impronta digitale" partendo dal modello non [… sia] possibile, nemmeno conoscendo l'algoritmo di elaborazione" (cfr. nota del XX), si osserva quanto segue.

Le informazioni trattate per il tramite di tale sistema risultano comunque riconducibili ad un codice direttamente identificativo del singolo dipendente, ne consentono o confermano l'identificazione univoca e costituiscono pertanto dati personali biometrici (cfr. art. 4, nn. 1) e 14), del Regolamento).

Ciò premesso, si fa presente che la finalità di rilevazione delle presenze in servizio dei dipendenti, funzionale all'attestazione dell'osservanza dell'orario di lavoro alla sua contabilizzazione, che, in generale, nell'ambito del pubblico impiego, è prevista da un quadro normativo stratificatosi nel tempo (v. ad esempio, art. 22, comma 3 della l. 23.12.1994, n. 724; art. 3 della l. 24.12.2007, n. 244; art. 7 del d.P.R. 1.02.1986, n. 13), è riconducibile nell'ambito di applicazione dell'articolo 9 par. 2, lett. b) del Regolamento poiché implica 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 […]" (v. pure art. 88, par. 1, Regolamento). Tuttavia, l'impiego di sistemi di rilevazione delle presenze che comportano anche il trattamento di dati biometrici richiede, nel sistema del Regolamento e del Codice, un'espressa previsione normativa e specifiche garanzie per i diritti degli interessati (il trattamento è infatti consentito "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), del Regolamento e cons. 51-53, e "nel rispetto delle misure di garanzia" individuate dal Garante ai sensi dell'art. 9, par. 4, del Regolamento e dell'art. 2-septies del Codice).

Nel contesto lavorativo il trattamento avente a oggetto dati biometrici può essere lecitamente posto in essere solo ove lo stesso trovi il proprio fondamento in una disposizione normativa che possa essere ritenuta base giuridica del trattamento "idonea" anche alla luce dell'assetto delle fonti dell'"ordinamento costituzionale" dello Stato membro (v. considerando 41 del Regolamento e v. anche Corte Cost. sent. n. 271/2005, in base alla quale la disciplina di protezione dei dati personali rientra fra la materia di competenza esclusiva statale riferita all'"ordinamento civile"). Tale disposizione deve, infatti, avere le caratteristiche richieste dalla disciplina di protezione dei dati e soddisfare specifici requisiti, sia in termini di qualità della fonte, contenuti necessari e misure appropriate e specifiche per tutelare i diritti e le libertà degli interessati, sia in termini di proporzionalità dell'intervento regolatorio rispetto alle finalità che si intendono perseguire (art. 6, parr. 2 e 3, lett. b), del Regolamento). Ciò in quanto, la base giuridica del trattamento, per poter essere considerata una valida condizione di liceità del trattamento, deve, tra l'altro, "persegu[ire] un obiettivo di interesse pubblico ed [essere] proporzionato all'obiettivo legittimo perseguito" (art. 6, par. 3, lett. b), del Regolamento).

Al riguardo, si fa presente inoltre che l'art. 2 della l. 19 giugno 2019, n. 56, recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo", aveva previsto una generalizzata sostituzione dei sistemi di rilevazione automatica delle presenze con sistemi di rilevazione di dati biometrici unitamente all'impiego di sistemi di videosorveglianza prevedendo che, "ai fini della verifica dell'osservanza dell'orario di lavoro", le amministrazioni pubbliche - individuate ai sensi dell'art. 1, comma 2, del d.lgs. n. 165/2001, ad esclusione del "personale in regime di diritto pubblico" (cfr. art. 3, comma 2, d.lgs. n. 165/2001), e quello sottoposto alla disciplina del lavoro agile di cui all'articolo 18 della legge 22 maggio 2017, n. 81 - "introducono sistemi di identificazione biometrica e di videosorveglianza in sostituzione dei diversi sistemi di rilevazione automatica attualmente in uso" ma prevede anche che le "modalità attuative" della norma – nel rispetto dell'art. 9 del Regolamento e delle misure di garanzia definite dal Garante ai sensi dell'art. 2-septies del Codice – siano individuate con d.P.C.M., su proposta del Ministro della funzione pubblica, previa intesa con la conferenza unificata (stato regioni e autonomie locali) e "previo parere del Garante ai sensi dell'art. 154 del Codice sulle modalità del trattamento dei dati biometrici".

Nell'esercizio dei propri poteri consultivi sugli atti normativi (artt. 36, par. 4 e 58, par. 3 del Regolamento nonché art. 154 del Codice), il Garante aveva, a suo tempo, segnalato al legislatore nazionale le criticità della norma evidenziando, in particolare, "l'eccedenza rispetto alle finalità che si intendono perseguire, anche sotto il profilo della gradualità delle misure limitative che possono essere adottate nei confronti dei lavoratori" (cfr. provv. 11 ottobre 2018, n. 464, doc. web n. 9051774) e - confermando quanto già rilevato nel corso delle audizioni dinanzi alle Commissioni

parlamentari competenti (audizioni presso le Commissioni riunite I e XI, Affari Costituzionali e Lavoro, della Camera dei Deputati il 6 febbraio 2019, doc. web n. 9080870) -, ha ribadito, anche in relazione allo schema di regolamento di attuazione, peraltro mai adottato, che "non può ritenersi in alcun modo conforme al canone di proporzionalità- come declinato dalla giurisprudenza europea e interna– l'ipotizzata introduzione sistematica, generalizzata e indifferenziata per tutte le pubbliche amministrazioni di sistemi di rilevazione biometrica delle presenze, in ragione dei vincoli posti dall'ordinamento europeo sul punto, a motivo dell'invasività di tali forme di verifica e delle implicazioni derivanti dalla particolare natura del dato" (provv. 19 settembre 2019, n. 167, doc. web n. 9147290).

Le disposizioni che prevedevano l'introduzione di sistemi di rilevazione biometrica delle presenze, in ambito pubblico, contenute nei commi da 1 a 4 dell'art. 2 della l. 19 giugno 2019, n. 56, sono state da ultimo abrogate dalla l. 30 dicembre 2020, n. 178 (c.d. Legge di Bilancio 2021, art. 1, comma 958).
Per tali ragioni, si evidenzia che, in assenza di specifiche disposizioni che prevedano il trattamento dei dati biometrici per finalità di rilevazione delle presenze e delle relative garanzie, il relativo trattamento non può essere lecitamente effettuato, non sussistendo base giuridica.

In tale quadro, il Garante in numerosi casi ha accertato l'illiceità del trattamento dei dati biometrici dei dipendenti per la finalità di rilevazione delle presenze posto in essere da soggetti pubblici e privati in violazione degli artt. 5, par. 1, lett. a), 6 e 9 del Regolamento, adottando i conseguenti provvedimenti correttivi e sanzionatori (provv. 15 dicembre 2022, n. 422, doc. web n. 9852776; provv. 15 dicembre 2022, n. 423, doc. web n. 9852800; provv. 14 gennaio 2021, n. 16, doc. web n. 9542071; per analoghe considerazioni in ambito privato, cfr. provv. 22 febbraio 2024, n. 105, 106, 107, 108 e 109, doc. web nn. 9995680, 9995701, 9995741, 9995762, 9995785; provv. 10 novembre 2022, n. 369, doc. web n. 9832838).

Nei menzionati provvedimenti, il Garante ha altresì avuto modo di chiarire come il difetto di base giuridica, in merito al trattamento dei dati biometrici, non possa essere colmato neppure dal consenso dei dipendenti, che l'Istituto ha dichiarato di aver acquisito nel caso di specie, assicurando altresì ai dipendenti che non lo avessero rilasciato la possibilità di attestare la propria presenza in servizio senza conferire a tal fine dati biometrici. Ciò in quanto, 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, il consenso 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 (cons. n. 43; art. 4, punto 11), e art. 7, par. 3 e 4, del Regolamento; v., l'orientamento consolidato in sede europea, Gruppo di lavoro "Articolo 29", Parere 2/2017 sul trattamento dei dati sul posto di lavoro, WP 249, p. 7 e 26 e Linee Guida sul consenso ai sensi del Regolamento UE 2016/679- WP 259- del 4 maggio 2020).

Per le ragioni che precedono, deve concludersi che il trattamento dei dati personali biometrici dei dipendenti amministrativi, tecnici e ausiliari (A.T.A.), effettuato dall'Istituto al fine di identificarli in modo univoco per rilevarne la presenza in servizio, è stato posto in essere in maniera non conforme al principio di "liceità, correttezza e trasparenza" nonché in assenza di un idoneo presupposto normativo, in violazione degli artt. 5, par. 1, lett. a), 6 e 9 del Regolamento

5. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice , seppure meritevoli di considerazione, non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano insufficienti a consentire l'archiviazione del presente procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art.

11 del Regolamento del Garante n. 1/2019.

Si confermano, pertanto, le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato dall'Istituto, per aver effettuato il predetto trattamento in violazione degli artt. 5, par. 1, lett. a), 6 e 9 del Regolamento.

Tenuto conto che la violazione delle predette disposizioni ha avuto luogo in conseguenza di un'unica condotta (stesso trattamento o trattamenti tra loro collegati), trova applicazione l'art. 83, par. 3, del Regolamento, ai sensi del quale l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. Considerato che, nel caso di specie, le violazioni sono soggette alla sanzione prevista dall'art. 83, par. 5, del Regolamento, l'importo totale della sanzione è da quantificarsi fino a euro 20.000.000.

In tale quadro, considerando, in ogni caso, che la condotta ha esaurito i suoi effetti - atteso che l'Istituto ha dichiarato di aver sospeso l'utilizzo del sistema di rilevazione biometrica delle presenze dei dipendenti A.T.A. nel XX nonché di aver cancellato i dati biometrici precedentemente raccolti - non ricorrono i presupposti per l'adozione di ulteriori misure correttive di cui all'art. 58, par. 2, del 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).

Il Garante, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso" e, in tale quadro, "il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, nel caso di specie la violazione delle disposizioni citate è soggetta all'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento.

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenendo in debito conto gli elementi previsti dall'art. 83, par. 2, del Regolamento.

Tenuto conto, in particolare, che:

- il trattamento, che ha riguardato unicamente i dipendenti A.T.A. (34 persone), ai quali era comunque riconosciuta la possibilità di registrare la propria presenza in servizio attraverso modalità tradizionali che non comportavano il trattamento di dati biometrici (art. 83, par. 2, lett. a), del Regolamento);

- il titolare, nel fare affidamento sulle informazioni rese dalla società fornitrice del sistema, ha ritenuto di non consultare il proprio responsabile della protezione dei dati, iniziativa che avrebbe invece consentito allo stesso di avvedersi degli specifici ed elevati rischi per i diritti e le libertà degli interessati coinvolti e di orientare le proprie scelte al riguardo in maniera maggiormente consapevole e, se del caso, diversa (art. 83, par. 2, lett. b), del Regolamento);

- il trattamento ha avuto ad oggetto dati biometrici intesi ad identificare in modo univoco gli

interessati di cui agli artt. 4, n. 14), del Regolamento, dati che, analogamente a quelli sulla salute e genetici, sono tutelati in maniera particolarmente stringente dal Regolamento e dal Codice (cfr. art. 83, par. 2, lett. g), del Regolamento),

si ritiene che, nel caso di specie, il livello di gravità della violazione commessa dal titolare del trattamento sia alto (cfr. Comitato europeo per la protezione dei dati, "Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR" del 24 maggio 2023, punto 60).

Ciò premesso, nel tenere presente che, comunque, il titolare è costituito da un istituto scolastico, si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze attenuanti:

il titolare ha offerto una buona cooperazione con l'Autorità nel corso dell'istruttoria, avendo, peraltro, fornito tempestiva comunicazione delle iniziative intraprese per porre rimedio alla violazione (art. 83, par. 2, lett. f), del Regolamento);

non risultano precedenti violazioni pertinenti commesse dall'Istituto (art. 83, par. 2, lett. e), del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 4.000,00 (quattromila/00) per la violazione degli artt. 5, 6 e 9 del Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, 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 capo contenente l'ordinanza ingiunzione sul sito Internet del Garante. Ciò in considerazione della particolare natura dei dati personali oggetto di trattamento e dei connessi rischi per gli interessati nel contesto lavorativo.

Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

TUTTO CIÒ PREMESSO IL GARANTE

dichiara, ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, l'illiceità del trattamento effettuato dall'Istituto di Istruzione Superiore "P. Galluppi" Tropea per violazione degli artt. 5, 6 e 9 del Regolamento, nei termini di cui in motivazione;

ORDINA

all'Istituto di Istruzione Superiore "P. Galluppi" Tropea in persona del legale rappresentante pro-tempore, con sede legale in viale Coniugi Crigna snc - 89861 Tropea (VV), C.F. 96012510796, di pagare la somma di euro 4.000,00 (quattromila/00) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione. Si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

al predetto Istituto, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 4.000,00 (quattromila/00) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

DISPONE

- ai sensi dell’art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, la pubblicazione dell’ordinanza ingiunzione sul sito internet del Garante;

- ai sensi dell’art. 154-bis, comma 3 del Codice e dell’art. 37 del Regolamento del Garante n. 1/2019, la pubblicazione del presente provvedimento sul sito internet dell’Autorità;

- ai sensi dell’art. 17 del Regolamento del Garante n. 1/2019, l’annotazione delle violazioni e delle misure adottate in conformità all’art. 58, par. 2 del Regolamento, nel registro interno dell’Autorità previsto dall’art. 57, par. 1, lett. u) del Regolamento.

Ai sensi degli artt. 78 del Regolamento, 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento è possibile proporre ricorso dinnanzi all’autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all’estero.

Roma, 27 marzo 2025

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei