Ordinanza ingiunzione nei confronti di Azienda sanitaria provinciale di Enna - 14 gennaio 2021 [9542071]

VEDI ANCHE NEWSLETTER DEL 19 FEBBRAIO 2021

[doc. web n. 9542071]

Ordinanza ingiunzione nei confronti di Azienda sanitaria provinciale di Enna - 14 gennaio 2021

Registro dei provvedimenti
n. 16 del 14 gennaio 2021

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 del n. 98 del 4/4/2019, pubblicato in G.U. n. 106 dell'8/5/2019 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. Premessa.

In riferimento ad articoli di stampa pubblicati nel novembre 2019 che riportavano la notizia che l'Azienda sanitaria provinciale di Enna (di seguito "l'Azienda") aveva adottato, nelle proprie sedi, un sistema che consente il trattamento dei dati biometrici dei dipendenti per la rilevazione delle presenze, al fine di garantire "una maggiore affidabilità tecnica nella verifica dell'identità di ogni dipendente" e "scoraggia[re] fenomeni di assenteismo […]", l'Ufficio ha avviato un'istruttoria nei confronti dell'Azienda.

2. L'attività istruttoria.

In riscontro alle specifiche richieste dell'Ufficio (cfr. nota del XX, prot. n. XX in atti), l'Azienda, con nota del XX, ha precisato che:

- la stessa "eroga le proprie prestazioni in 21 Comuni appartenenti alla provincia di Enna e […] di Messina. I dipendenti dell'azienda […] sono oltre 2000 e prestano servizio in 4 presidi ospedalieri […] nonché presso gli ambulatori e i presidi territoriali allocati in 22 Comuni";

- l'amministrazione ha introdotto "il sistema di verifica biometrica dell'identità" in quanto "l'esistenza di presidi decentrati […] e la tipologia dell'attività prestata (diversi operatori prestano la propria attività su due e/o tre turni nelle 24 ore, talvolta anche in presidi ospedalieri e territoriali) comporta una notevole complessità nella gestione del personale dipendente" e pertanto il sistema è stato attivato "alla luce di quanto previsto dalla legge n. 56/2019";

- il sistema utilizza "un software in grado di acquisire i dati dello stesso dipendente e memorizzarli in forma crittografata su un dispositivo sicuro (badge) dato nell'esclusiva disponibilità dell'interessato";

- "il software provvede, immediatamente dopo la fase di registrazione in forma crittografata dei dati, alla loro cancellazione";

- "a tutti i dipendenti è stata fornita l'informativa ai sensi dell'art. 13 del Regolamento";

- la procedura di registrazione del dato comporta la "rilevazione dell'impronta biometrica che viene trasformata in una stringa criptata, memorizzata a sua volta nel badge"

- la lettura del dato, all'atto della rilevazione della presenza, avviene mediante contestuale utilizzo del badge (che deve essere avvicinato al rilevatore delle presenze) e mediante apposizione del dito sul dispositivo: "il sistema confronta localmente e solo per il tempo necessario alla verifica, stringa conservata nel badge con quella calcolata momentaneamente dal rilevatore delle presenze" e, se il confronto è coincidente, "la stringa calcolata momentaneamente viene automaticamente cancellata […] nessun dato biometrico viene memorizzato", ma "solo il numero di matricola del dipendente, l'ora e la data di presenza";

- "nessun sistema di videosorveglianza è stato installato nei vari accessi aziendali"; e per tutte queste ragioni l'Azienda sostiene che "non sussistono criticità, né violazioni di norme". Tali considerazioni sono contenute anche in un documento denominato "valutazione di impatto".

Con nota del XX (prot. n. XX), l'Ufficio, sulla base degli elementi acquisiti, ha notificato all'Azienda, 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, invitando il predetto titolare 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, dalla legge n. 689 del 24/11/1981).

Con la nota sopra menzionata, l'Ufficio ha rilevato che l'Azienda tratta, con le modalità sopra descritte, dati biometrici dei dipendenti per la finalità di rilevazione delle presenze in violazione del principio di "liceità, correttezza e trasparenza", art. 5, par. 1, lett. a), del Regolamento e in assenza di un idoneo presupposto di liceità, in violazione degli artt. 6, par. 1, lett. c) e 9 par. 2, lett. b), e par. 4, del Regolamento.

Con nota del XX l'Azienda ha fatto pervenire le proprie memorie difensive, rappresentando, tra l'altro, che:

- non sussisterebbe alcun trattamento di dati personali da parte dell'amministrazione in quanto "il trattamento dei dati personali propri dell'interessato [sarebbe] effettuato da questo stesso" e "deve considerarsi in sé lecito e legittimo ai sensi dell'ordinamento nazionale e di quello comunitario, senza che ad esso debbano (o possano) essere applicate i presupposti e le eventuali limitazioni sancite dagli articoli 5. 6 e 9 del Regolamento", analogamente a quanto avviene per "il trattamento dell'impronta digitale propria memorizzata su uno specifico device, come strumento di accesso allo stesso (che si tratti dell'elaboratore o dello smartphone proprio del soggetto in questione) [che] esula da qualsiasi applicazione della normativa nazionale e comunitaria" (cfr. pp. 4 e 5);

- "nel caso di specie sussistono certamente tutte le condizioni per concludere che, nel momento in cui viene effettuata la verifica dell'identità del dipendente ai varchi di accesso, vi sia effettivamente un trattamento di dati personali biometrici [ma che lo stesso non sia] soggetto alle norme del Regolamento e del Codice" ed esuli "conseguentemente dalla competenza

dell'Autorità Garante;

- ciò in quanto "il trattamento è effettuato direttamente e personalmente dall'interessato […] l'intero meccanismo risulta predisposto appositamente in modo da evitare che un soggetto diverso dall'interessato possa effettuare il trattamento dei dati biometrici dell'interessato medesimo […] il trattamento del dato biometrico ha inizio (in modo automatizzato) se e quando (e solo quando) il dipendente da inizio al procedimento stesso compiendo due operazioni materiali che sono sotto il suo personale ed esclusivo controllo: a. L'appoggio del badge sul lettore e b. L'appoggio del polpastrello sullo scanner. Dopo il compimento di tali operazioni ha inizio il procedimento di rilievo e confronto dei dati" (pp. 7 ss.)

- "tali semplici gesti hanno un significato univoco espressivo di una precisa volontà del dipendente di dare avvio e quindi, in un certo senso, di acconsentire al trattamento dei dati";

- "durante il confronto tra il dato biometrico memorizzato e quello rilevato dallo scanner, il lettore non comunica con altri sistemi o macchine e non vi è dunque possibilità che i dati biometrici che in quel momento si trovano (sebbene per pochissimi istanti) all'interno della macchina siano acquisiti, memorizzati, alterati, o trattati in qualsiasi modo da soggetti terzi. Per fare ciò sarebbe, infatti, necessario accedere fisicamente alla macchina in quello stesso breve lasso temporale in cui avviene il confronto dei dati – lasso temporale in cui, però, l'interessato al trattamento si trova direttamente a contatto fisico con la macchina medesima che è, quindi, sotto il suo diretto controllo";

- "l'intero processo di trattamento del dato biometrico non avviene mai e non può mai avvenire sotto il controllo diretto o indiretto dell'amministrazione perché esso avviene sotto il diretto ed esclusivo controllo del dipendente ed è, anzi, espressamente finalizzato ad impedire che altri soggetti che non siano l'interessato possano avere qualunque accesso ai dati personali e biometrici dello stesso" (p. 9);

- in ogni caso - ove si ritenesse che il trattamento rientri nell'ambito di applicazione del Regolamento- "la finalità perseguita dall'adozione dei sistemi biometrici di rilevazione delle presenze risponde ad un'esigenza di estrema attualità volta alla prevenzione di reati contro la pubblica amministrazione e, in generale di comportamenti scorretti da parte dei dipendenti, di per sé idonei a ridurre considerevolmente l'efficienza della Pubblica Amministrazione. Laddove, come nel caso di specie, la pubblica Amministrazione interessata operi nel campo dell'assistenza sanitaria vengono quindi in rilievo due distinti interessi cardine dell'ordinamento tanto nazionale (art. 32 ed art. 97 Costituzione della Repubblica) che comunitario (artt. 35 e art. 41 della Carta dei Diritti Fondamentali dell'Unione Europea): il diritto alla salute ed il principio del buon andamento dell'amministrazione" (p.11);

- "negli ultimi anni, svariate amministrazioni pubbliche hanno compiuto la medesima scelta di adozione di un sistema di verifica biometrica delle presenze senza andare incontro, per quanto ne possa sapere l'Azienda deducente, ad alcuna contestazione da parte della predetta Autorità […] da indurre nella generale convinzione della liceità del comportamento […] "il Garante della privacy, con provvedimento del 15 settembre 2016 n. 357, esprimeva parere positivo con riferimento alla richiesta preliminare [di un'azienda ospedaliera …] per l'installazione del sistema di lettura di dati biometrici (impronte digitali) per la rilevazione della presenza in servizio dei dipendenti […con] modalità di funzionamento [analoghe a quelle in uso] presso l'ASP di Enna" (p. 16);

- "la sussistenza di un obbligo legale risalente alla l. 56/2019 […pur se oggetto] di numerosi rilievi critici circa la compatibilità di tale norma nazionale con il contesto normativo comunitario […] porta a escludere che nel caso di specie possa essere imputata all'ASP di Enna una violazione dell'art. 6";

- "l'amministrazione interessata, dunque, non può che adeguarsi a quello che (la stessa Autorità Garante) ritiene essere un obbligo normativamente imposto a fronte della sussistenza di meri dubbi sulla compatibilità di detto obbligo con alcuni dei criteri dettati dal Regolamento (dubbi che peraltro l'Amministrazione non ritiene di poter condividere se non nei limiti in cui riguardano modalità di rilevamento diverse da quelle prese in esame in questa sede). Il sistema di rilevamento delle presenze adottato si è infatti in tutto e per tutto adeguato alle modalità operative suggerite nel predetto parere";

- "la presenza effettiva in servizio dei pubblici dipendenti e la conseguente effettiva esecuzione delle mansioni loro attribuite costituiscono condizione essenziale per il perseguimento dell'obiettivo del buon andamento della pubblica amministrazione. Di conseguenza, sono palesi la ricorrenza del parametro prescritto dalla lett. e) dell'art. 6 del Regolamento e la

conseguente liceità del trattamento di dati biomedici in questione [anche alla luce] della lettera f) dell'art. 6 del Regolamento" (p. 21)

- quanto alla violazione dell'art. 9, par. 2 lett. b), del Regolamento "è evidente che il sistema di verifica biometrica delle presenze sia stato adottato dall'ASP di Enna in quanto espressamente previsto come obbligo del datore di lavoro pubblico posto a suo carico della l. n.56/2019 […]" e "il trattamento in oggetto risulta peraltro necessario all'esercizio di diritti specifici del titolare del trattamento in materia di diritto del lavoro" tanto anche in ragione dei casi di "assenteismo verificatisi nell'Ospedale Chiello di Piazza Armerina, Presidio Ospedaliero rientrante nella competenza dell'ASP di Enna";

- il trattamento troverebbe inoltre la propria base giuridica anche nell'art. 9, par. 2 lett. g) e art. 2 sexies del codice lett. u) "compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica", compiti precipui, appunto, di un'Azienda sanitaria territoriale quale l'ASP di Enna" (p. 26);

- "nel predisporre il sistema che consentisse il rilievo biometrico ai varchi di ingresso, come previsto dalla normativa vigente, l'Azienda ha ritenuto di adeguarsi alle modalità risultanti dalle precedenti indicazioni di questa Autorità Garante, prima di tutto non predisponendo alcun contestuale sistema di rilievo audiovisivo in corrispondenza dei varchi. Questa Azienda, comprende e condivide le preoccupazioni che codesta Autorità Garante ha espresso nel proprio parere sullo schema di regolamento attuativo della. 56/2019" ma "non ritiene condivisibile la considerazione ivi espressa, secondo la quale l'incompatibilità delle disposizioni di cui all'art. 2 della legge n.56 non sarebbe sanabile con l'adozione di particolari modalità attuative dell'obbligo ivi sancito, poiché essa risiederebbe 'nell'an prima che nel quomodo del trattamento'";

- "A fronte del diritto di libertà costituito dalla tutela dei dati personali (ed in particolare dei dati biometrici) garantito dalla normativa nazionale e comunitaria vi sono interessi pubblici molteplici e non subordinati ma pari ordinati rispetto ad esso. La valutazione di tali interessi pubblici e la scelta di tutelarli attraverso l'imposizione di un obbligo generalizzato compete al legislatore ordinario nazionale, anche perché in questi termini si esprime lo stesso Regolamento. La valutazione di proporzionalità del trattamento, quindi, si deve spostare proprio sul contenuto e sulle modalità del trattamento stesso, senza, peraltro, dimenticare che lo stesso articolo 2 della l.56/2019 richiama tale principio come criterio orientativo dell'applicazione dell'obbligo di legge" (pp. 30 e 31);

- "si ritiene comunque che debba applicarsi alla condotta tenuta da questa Azienda l'esimente dell'errore scusabile che la giurisprudenza riconosce in applicazione dell'art. 3 l.689\1981 [...]" in quanto "da una parte il legislatore che ha introdotto l'obbligo generalizzato di rilievo delle presenze attraverso la rilevazione di dati biometrici. […] Dall'altra parte la condotta di codesta stessa Autorità Garante che: prima dell'introduzione del G.D.P.R. ha consentito espressamente a soggetti pubblici svolgenti le medesime funzioni di questa Azienda e per finalità analoghe a quelle dalla stessa perseguite di introdurre un sistema di rilevazione generalizzata delle presenze mediante verifica dei dati biometrici, dopo l'introduzione del G.D.P.R. non ha – per quanto risulta – disposto sanzioni o divieti a carico di questi medesimi enti per le stesse ragioni ora oggetto di contestazione […]";

- "l'amministrazione ha richiesto ed ottenuto dal legale rappresentante della ditta appaltatrice (doc.1) prima di procedere all'istallazione del sistema in questione e che attesta, sotto la penale e personale responsabilità del dichiarate la conformità del sistema stesso alla legge ed al parere di questa Autorità";

- è stato inoltre chiarito che "l'operatività del sistema risulta attualmente sospesa in esito alle contestazioni del Garante".

3. Esito dell'attività istruttoria.

La disciplina di protezione dei dati personali prevede che il datore di lavoro può trattare i dati personali, anche relativi a categorie particolari di dati (cfr. art. 9, par. 1 del Regolamento), dei dipendenti se il trattamento è necessario, in generale, per la gestione del rapporto di lavoro e per adempiere a specifici obblighi o compiti previsti da leggi, dalla normativa comunitaria, da regolamenti o da contratti collettivi (artt. 6, par. 1, lett. c), 9, parr. 2, lett. b), e 4, e 88 del Regolamento).

Il trattamento è, inoltre, lecito quando sia "necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" ovvero, quando "necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza

del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato" (artt. 6, parr. 1, lett. e), 2 e 3, nonché 9, par. 2, lett. g,) del Regolamento e 2-ter e 2-sexies del Codice).

Il legislatore nazionale ha definito "rilevante" l'interesse pubblico per il trattamento "effettuato da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri" nelle materie indicate, seppur in modo non esaustivo, dall'art. 2-sexies del Codice, stabilendo che i relativi trattamenti "sono ammessi qualora siano previsti […] da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato".

Come noto, la definizione di dati biometrici li individua 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 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.

In tale quadro, il trattamento di dati biometrici (di regola vietato) è consentito 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 "liceità, correttezza e trasparenza", "limitazione delle finalità", "minimizzazione" nonché "integrità e riservatezza" dei dati e "responsabilizzazione" (art. 5 del Regolamento). I dati devono, inoltre, essere "trattati in maniera da garantire un'adeguata sicurezza" degli stessi, "compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali" (art. 5, par. 1, lett. f), e art. 32 del Regolamento).

3.1. L'applicabilità del quadro normativo in materia di protezione dei dati al trattamento dei dati biometrici effettuato dall'Azienda.

Occorre preliminarmente evidenziare che il trattamento di dati personali consiste in una "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione" (art. 4, punto 2), del Regolamento).

Sebbene l'Azienda ammetta che "nel momento in cui viene effettuata la verifica dell'identità del dipendente ai varchi di accesso, vi sia effettivamente un trattamento di dati personali biometrici", la stessa ritiene che "questo particolare trattamento esuli dall'applicazione della normativa del Regolamento comunitario, nonché, conseguentemente, dalla competenza di questa Autorità Garante", in ragione del fatto che "il trattamento è effettuato direttamente e personalmente dall'interessato e quindi non soggetto all'applicazione dei principi di liceità e correttezza sanciti dagli artt. 5-6-9 del Regolamento" (cfr. nota del XX, pp. 6 e 7).

Sulla base degli elementi sopra riportati, deve invece ritenersi che, contrariamente a quanto sostenuto dall'Azienda, le operazioni sopra descritte diano luogo comunque a un trattamento di dati biometrici da parte della stessa Azienda, soggetto all'applicazione del quadro normativo in materia di protezione dei dati personali.

Nel caso in esame infatti l'Azienda – ancorché non conservi su una banca dati centralizzata i dati biometrici degli interessati, ma

solo su dispositivi portatili dotati di adeguate capacità crittografiche (badge con funzionalità di smart card), affidati alla diretta ed esclusiva disponibilità di ciascun interessato – effettua comunque trattamenti di dati biometrici che, come confermato dall'Azienda, "si trovano (sebbene per pochissimi istanti) all'interno" di sistemi impiegati dal datore di lavoro per la rilevazione delle presenze e per le connesse finalità di gestione del rapporto contrattuale con i propri dipendenti. Ciò, sia nella fase di registrazione (c.d. enrollment) con l'acquisizione delle caratteristiche biometriche (impronte digitali) dell'interessato (v. anche punti 6.1 e 6.2 dell'allegato A al provvedimento del Garante del 12 novembre 2014, n. 513), sia nella fase di riconoscimento biometrico, all'atto delle rilevazioni delle presenze (v. anche punto 6.3 dell'allegato A al citato provvedimento).

Tali trattamenti sono, infatti, funzionali a consentire la rilevazione dei dati di entrata e uscita dei dipendenti ai fini dell'attestazione dell'osservanza dell'orario di lavoro e per la relativa contabilizzazione, finalità 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), non potendo gli stessi essere, in alcun modo, assimilati a quelli compiuti dall'interessato per accedere a un proprio dispositivo mobile "per l'esercizio di attività a carattere esclusivamente personale o domestico" (art. 2, par. 2, lett. c), e cons. n. 18 del Regolamento).

In particolare, nella fase di registrazione, l'Azienda acquisisce, tramite un apposito lettore, l'impronta digitale dell'interessato, al fine di creare un modello biometrico (ossia una descrizione informatica sintetica della caratteristica biometrica ottenuta estraendo dal campione biometrico soltanto gli elementi salienti predefiniti) che viene memorizzato, in modo sicuro, all'interno del badge consegnato all'interessato.

Nelle successive fasi di riconoscimento biometrico dell'interessato, l'Azienda verifica l'identità dello stesso mediante il confronto tra il modello biometrico di riferimento, memorizzato all'interno del badge, e il modello biometrico ricavato dall'impronta digitale presentata all'atto del rilevamento della presenza. Qualora l'operazione di confronto vada a buon fine, l'identità dell'interessato può dirsi verificata e vengono tramessi, al sistema di gestione delle presenze, il numero di matricola del dipendente unitamente ad altre informazioni (quali la data e l'ora della timbratura).

La conservazione dei dati biometrici, con modalità sicure su badge con funzionalità di smart card che l'amministrazione affida all'esclusiva disponibilità di ciascun interessato, risponde a una scelta progettuale del titolare che, al momento di determinare i mezzi del trattamento, adotta tale misura tecnica e organizzativa in attuazione del principio di minimizzazione dei dati oggetto di trattamento (cfr. artt. 5, par. 1, lett. c), 24 e 25 del Regolamento), restando però, in ogni caso, necessaria la preliminare verifica in ordine alla ricorrenza dei presupposti di liceità per trattare i dati biometrici dei dipendenti (art. 9 del Regolamento). Si osserva infatti che, anche nel previgente quadro normativo, tale modalità di conservazione dei dati biometrici era stata espressamente indicata dal Garante tra le misure e accorgimenti di carattere tecnico che, sempre in presenza delle condizioni di liceità del trattamento (al tempo, notificazione e istanza di verifica preliminare al Garante, salva la ricorrenza di specifiche ipotesi di esonero, cfr. par. 4, provv. 12 novembre 2014, n. 513), il titolare doveva adottare per garantire la proporzionalità e la sicurezza del trattamento.

Per tali ragioni, l'adozione di questa misura non esclude, anzi conferma, l'applicazione della disciplina in materia di protezione dei dati personali ai trattamenti in esame, come peraltro comprovato anche dal fatto che l'Azienda ha ritenuto necessario assolvere l'obbligo di rendere agli interessati un'informativa, nell'imminenza dell'attivazione del nuovo sistema di rilevazione delle presenze.

3.2. La correttezza e trasparenza del trattamento: l'informativa agli interessati.

Il titolare del trattamento deve trattare i dati "in modo lecito, corretto e trasparente nei confronti dell'interessato" (art. 5, par. 1, lett. a) del Regolamento), adottando "misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 […]" (art. 12 del Regolamento).

Sebbene l'Azienda abbia assicurato, in un primo momento, che "a tutti i dipendenti è stata fornita l'informativa ai sensi dell'art. 13 del Regolamento" (cfr. nota del XX, cit.), tuttavia la stessa ha trasmesso la documentazione con la quale ritiene di aver assolto al predetto obbligo solo successivamente, su sollecitazione dell'Ufficio, in allegato alle memorie difensive (cfr. all. n. XX, nota XX, cit.).

Dall'esame di tale documentazione, emerge che l'Azienda ha certamente avvertito il personale e informato le organizzazioni sindacali della scelta organizzativa compiuta, diramando a tal fine talune note e documenti che contengono generici riferimenti, in nessuno dei quali sono però riportate tutte le informazioni richieste dal Regolamento per assicurare un trattamento corretto e

trasparente (art. 13 del Regolamento).

Sempre sotto il profilo della correttezza e trasparenza, si rileva inoltre che, in tali note e documenti, il trattamento viene prospettato come pienamente conforme al quadro normativo in materia di protezione dei dati e alle indicazioni fornite dal Garante.

In particolare, si osserva che la nota indirizzata a tutto il personale, in data XX (all. n. XX, nota del XX, in atti), "integrata dalle istruzioni affisse in prossimità dei rilevatori", si limita a indicare che "in applicazione dell'art. 2 della legge n. 56 del 19.6.2019 con decorrenza dal 4 novembre 2019 entrerà in funzione il nuovo sistema di rilevazione delle presenze mediante l'utilizzo del sensore biometrico" […ciò] nel pieno rispetto della vigente normativa in materia di dati personali, stante che, tali dati, rimangono memorizzati solo sul tesserino personale, in possesso del solo dipendente". Peraltro in altro documento, denominato "Informativa sui sistemi di rilevazione di identità biometrica", si dichiara che il sistema "è coerente con il Parere su uno schema di decreto del Presidente del Consiglio dei ministri concernente la disciplina di attuazione della disposizione di cui all'articolo 2 della legge 19 giugno 2019, n. 56, recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo" - 19 settembre 2019 perché l'impronta è criptata e memorizzata solo sul tesserino che resta in possesso del dipendente".

Per tali ragioni il trattamento risulta essere stato effettuato in violazione dei principi di liceità, trasparenza e correttezza (art. 5, par. 1, lett. a), del Regolamento) in quanto i documenti informativi, sopra indicati, non rappresentano compiutamente il trattamento effettuato, prospettandolo peraltro come conforme al quadro normativo in materia di protezione dei dati.

3.3. L'assenza di base giuridica per il trattamento di dati biometrici per finalità di rilevazione delle presenze.

Alla luce degli elementi acquisiti e delle dichiarazioni rese nel corso dell'istruttoria, è emerso che nel mese di XX (più specificatamente, come da documentazione in atti, a decorrere dal XX) l'Azienda ha attivato un sistema di rilevazione delle presenze che comporta il trattamento dei dati biometrici dei dipendenti.

Le ragioni che avrebbero reso necessaria l'introduzione del sistema sarebbero legate alla "notevole complessità nella gestione del personale dipendente" in ragione del numero di dipendenti ("oltre 2000") e della vastità dell'ambito territoriale in cui sono ubicati i presidi ospedalieri e ambulatoriali in cui prestano servizio ("allocati in 22 Comuni"); la scelta sarebbe inoltre avvenuta "alla luce di quanto previsto dalla legge n. 56/2019". Dalla documentazione in atti e da quanto ribadito nelle memorie difensive, emerge che l'amministrazione, nel dare corso al trattamento, abbia ritenuto che il consenso degli interessati costituisca idonea condizione di liceità del trattamento (cfr. Documento relativo alla Valutazione di impatto, allegato alla nota del XX, cit.).

In ogni caso l'Azienda ha provveduto a sospendere il trattamento in esito alle contestazioni del Garante: come risulta dagli atti è stato chiesto alla direzione competente di rivolgersi alla ditta fornitrice del servizio per il ripristino della "precedente modalità d'uso" del sistema di rilevazione delle presenze, disattivando la funzionalità di riconoscimento biometrico (cfr. nota XX, prot. XX, all. n. XX, in atti).

Nel corso dell'istruttoria l'Azienda ha rappresentato di essersi adeguata "alle modalità risultanti dalle precedenti indicazioni di questa Autorità Garante", menzionando, tra l'altro, il "provvedimento del 15 settembre 2016 n. 357 [con il quale il Garante] esprimeva parere positivo con riferimento alla richiesta preliminare [di un'azienda ospedaliera …] per l'installazione del sistema di lettura di dati biometrici (impronte digitali) per la rilevazione della presenza in servizio dei dipendenti" (cfr. p. 16, nota 17 febbraio cit.).

A tal proposto nel premettere che solo alcuni dei casi richiamati dall'Azienda sono stati sottoposti al Garante con istanze di verifiche preliminari, anteriormente all'entrata in vigore del Regolamento, appare necessario ricostruire il sistema delle basi giuridiche per il trattamento dei dati biometrici per i quali è prevista ora una tutela rafforzata rispetto al precedente quadro normativo (direttiva n. 95/46, legge n. 675/1996 e Codice).

Nel sistema previgente i dati biometrici non erano considerati "sensibili", eppure in considerazione della loro stretta e stabile relazione con l'individuo e la sua identità, i titolari pubblici o privati potevano iniziare il trattamento, salve specifiche ipotesi di esonero, previa notificazione e solo dopo aver sottoposto il trattamento alla verifica preliminare del Garante, quali condizioni di liceità del trattamento prima dell'inizio dello stesso (artt. 17 e 37, comma 1, lett. a) del Codice, nel testo antecedente alle modifiche del d.lgs. n. 101/2018; cfr. Provvedimento generale prescrittivo in tema di biometria, 12 novembre 2014, n. 513, doc. web n. 3556992, punto 4); provv. 23 novembre 2006, n. 53, doc. web n. 1364099 e provv. 14 giugno 2007, XX 23, doc. web n. 1417809;

nonché provv.ti 22 ottobre 2015, n. 552, doc. web n. 4430740 e 17 marzo 2016, n. 129, doc. web n. 4948405; più di recente, tali principi sono stati confermati con il provv. n. 249 del 24 maggio 2017, doc. web n. 6531525).

In questo delicato ambito, fin dal 2007 il Garante ha evidenziato che i principi di protezione dei dati impongono che siano preventivamente considerati altri sistemi, dispositivi e misure di sicurezza – meno invasive– che possano assicurare l'attendibile verifica delle presenze, senza fare ricorso al trattamento dei dati biometrici (v. già, Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro, rispettivamente, alle dipendenze di datori di lavoro privati e in ambito pubblico provv. 23 novembre 2006, n. 53, doc. web n. 1364099 e provv. 14 giugno 2007, n. 23, doc. web n. 1417809). Tali principi trovano conferma anche a livello internazionale e nelle posizioni assunte dalle altre autorità di controllo (v. Raccomandazione CM/Rec(2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale, par. 18; v. anche Gruppo di lavoro "Articolo 29", Parere 2/2017 sul trattamento dei dati sul posto di lavoro, WP 249, par. 5; CNIL, deliberazione 10.1.2019 https://www.cnil.fr/fr/biometrie-sur-les-lieux-de-travail-publication-dun-reglement-type e le FAQ pubblicate in data 28 marzo 2019 "Question-réponses sur le règlement type biométrie nonché le precedenti linee guida "Travail & données personnells").

In tale quadro, con riguardo ad alcuni casi di uso generalizzato dei sistemi biometrici nel contesto lavorativo, a fronte di generiche esigenze di prevenzione circa l'eventuale utilizzo distorto degli strumenti di rilevazione delle presenze d'uso comune (quali i badge), il Garante ha valutato non proporzionato il relativo trattamento (cfr., Provv.ti 30 maggio 2013 nn. 261 e 262 e 1° agosto 2013, n. 384, doc. web nn. 2502951, 2503101 e 2578547 nei confronti di alcuni istituti scolastici; ma anche 31 gennaio 2013, n. 38, doc. web n. 2304669 nei confronti di un Comune; v. anche il provv. n. 249 del 24 maggio 2017, doc. web n. 6531525, avente ad oggetto la carta multiservizi del Ministero della difesa), ammettendolo, invece, in limitate ipotesi e in presenza di obiettive e documentate esigenze che rendessero indispensabile l'adozione di tali sistemi, tenuto conto della specificità del caso concreto, del contesto socio-economico di riferimento e delle caratteristiche della tecnologia impiegata (cfr., ad esempio, provv. 15 settembre 2016 n. 357, doc. web n. 5505689, espressamente menzionato dall'Azienda nelle memorie difensive).

Il rafforzamento delle tutele dei dati biometrici previste nel Regolamento e nel Codice, come modificato dal d.lgs. n. 101/2018, mediante l'inclusione degli stessi nelle categorie di dati particolari, al pari dei dati sulla salute e genetici, tra quelle assistite cioè da un più elevato livello di garanzie (art. 9, par. 2 e par 4, del Regolamento), ha riguardato in primis i presupposti giuridici che rendono leciti i trattamenti di tali categorie di dati, prima ancora che gli aspetti di natura tecnica e le misure di sicurezza.

Nel contesto lavorativo, le finalità di rilevazione delle presenze dei dipendenti e di verifica dell'osservanza dell'orario di lavoro possono rientrare nell'ambito di applicazione dell'art. 9, par. 2, lett. b) del Regolamento in quanto implicanti 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]" (v. pure art. 88, par. 1, Regolamento), ovvero nell'ambito di applicazione dell'art. 9, par. 2, lett. g) del Regolamento, relativo al trattamento "necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato".

Nel primo caso, affine a quello di specie, il trattamento dei dati biometrici sarà 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 conss. nn. 51-53 del Regolamento),

In tale quadro, affinché uno specifico trattamento avente a oggetto dati biometrici possa essere lecitamente iniziato 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. 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).

L'art. 2 della legge 19 giugno 2019, n. 56, recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo", invocato dall'Azienda, ha previsto 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 – 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".

Come noto, l'iter normativo, indispensabile a integrare il sistema delle basi giuridiche del trattamento richiesto dal Regolamento e dal Codice con riguardo ai dati biometrici, non è stato, concluso -non essendo stato adottato il regolamento attuativo, che avrebbe dovuto contenere specifiche garanzie per circoscrivere e specificare la portata della norma nonché regolare le principali caratteristiche e modalità del trattamento- e, da ultimo, l'art. 1, comma 958 della legge 30 dicembre 2020, n. 178 (c.d. Legge di Bilancio 2021) ha abrogato i commi da 1 a 4 dell'articolo 2 della legge 19 giugno 2019.

A ciò si aggiunga che i provvedimenti con i quali il Garante ha espresso il dovuto parere sullo schema di disegno di legge e, successivamente, sullo schema di regolamento (cfr., provv. n. 464, 11 ottobre 2018, doc. web n. 9051774 e provv. n. 167 del 19 settembre 2019, doc. web n. 9147290), risultano peraltro, in larga parte, già noti all'Azienda, per averli espressamente menzionati nei documenti informativi diramati al personale e alle organizzazioni sindacali, prima di intraprendere il trattamento (cfr. all. n. XX, nota del XX).

Allo stato non sussiste pertanto un'idonea base giuridica che possa soddisfare i requisiti richiesti dal Regolamento e dal Codice per legittimare le amministrazioni pubbliche 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.

Le considerazioni che precedono valgono anche ove si ritenesse che la finalità perseguita dall'amministrazione, mediante il descritto trattamento, non sia solo quella connessa alla gestione del rapporto di lavoro ma anche quella di accrescere l'efficienza della pubblica amministrazione e perseguire il miglioramento dei servizi, mediante l'effettiva presenza in servizio delle risorse umane assegnate agli uffici pubblici (art. 97 Cost.), riconducendolo, come prospettato dall'Azienda, all'ambito dei trattamenti necessari per "motivi di interesse pubblico rilevante". Come noto, nel margine di flessibilità concesso al legislatore nazionale, la rilevanza dell'interesse pubblico è stata ulteriormente declinata nell'ambito dell'art. 2-sexies che ha specificato le condizioni, richieste dall'art. 9, par. 1, lett. g), del Regolamento, delimitando i presupposti di legittimità del trattamento, quando sono necessari per motivi di interesse pubblico rilevante, alla sussistenza di una previsione normativa che deve specificare, oltre al motivo di interesse pubblico rilevante, tra l'altro, i tipi di dati, le operazioni eseguibili, le misure appropriate per tutelare i diritti degli interessati. Tali elementi, allo stato, non sono stati individuati da alcuna disposizione normativa coerente col caso specifico di applicazione individuato dall'Azienda nei suoi scritti difensivi.

Né il difetto di base giuridica, in merito al trattamento dei dati biometrici, può essere superato dal consenso dei dipendenti posto che, come peraltro ribadito di recente dal Garante (da ultimo, provv. n. 35 del 13 febbraio 2020, doc. web n. 9285411) 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).

Da ultimo, contrariamente a quanto sostenuto dall'Azienda, il trattamento in esame non può essere lecitamente effettuato richiamando il legittimo interesse del titolare del trattamento, in quanto, non essendo indicato all'art. 9, par. 2, del Regolamento, lo stesso non può costituire idonea deroga al generale divieto di trattare categorie particolari di dati personali, né peraltro può trovare applicazione "al trattamento di dati effettuato dalle autorità pubbliche" (cfr. art. 6, par. 1, lett. f), del Regolamento).

Per tali ragioni, si ritiene che l'Azienda abbia effettuato dal 4 novembre 2019 il trattamento dei dati biometrici dei dipendenti per la finalità di rilevazione delle presenze in assenza di un'idonea base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6 e 9 del Regolamento.

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento negli scritti difensivi 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.

Il trattamento dei dati biometrici dei dipendenti dell’Azienda, avvenuto in violazione della disciplina in materia di trattamento dei dati personali è stato intrapreso, nel mese di novembre 2019, nella piena vigenza delle disposizioni del Regolamento e del Codice, come modificato dal d.lgs. n.101/2018. Per tali ragioni, al fine della determinazione del quadro normativo applicabile sotto il profilo temporale (art. 1, comma 2, della l. 24 novembre 1981, n. 689), queste costituiscono le disposizioni vigenti al momento della commessa violazione.

Si confermano pertanto le valutazioni preliminari dell’Ufficio e si rileva l’illiceità del trattamento di dati personali effettuato dall’Azienda, in quanto il trattamento dei dati biometrici degli interessati, è avvenuto in violazione dei principi generali del trattamento e in assenza di un’idonea base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6 e 9 del Regolamento.

La violazione delle predette disposizioni rende applicabile la sanzione amministrativa ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento medesimo come richiamato anche dall’art. 166, comma 2, del Codice.

5. Misure correttive (art. 58, par. 2, lett. d) del Regolamento).

Sebbene dal 23 gennaio 2020 l’Azienda abbia dato disposizioni per disattivare la funzionalità di riconoscimento biometrico all’atto della rilevazione delle presenze, non risulta in atti che i dati delle impronte digitali, memorizzati sotto forma di modello biometrico all’interno dei badge consegnati al personale, siano stati cancellati. Per tali ragioni il trattamento risulta ancora, seppur parzialmente, in corso.

In tale quadro, in ragione dell’illiceità del trattamento effettuato, si ritiene necessario disporre, ai sensi dell’art. 58, par. 2, lett. d), del Regolamento - che prevede che il Garante ha i poteri correttivi di “ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i travamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine” – la cancellazione dei dati personali (modelli biometrici) dei dipendenti attualmente memorizzati all’interno dei badge in uso agli stessi, entro sessanta giorni dalla notifica del presente provvedimento.

Ai sensi dell’art. 157 del Codice, l’Azienda dovrà, inoltre, provvedere a comunicare a questa Autorità le iniziative che intende intraprendere per assicurare la cessazione del trattamento entro trenta giorni dalla notifica del presente provvedimento.

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 – considerando anche il richiamo contenuto nell’art. 166, comma 2, del Codice – la violazione delle disposizioni citate è soggetta all’applicazione della stessa 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.

Si rileva preliminarmente che la condotta dell’Azienda non può essere considerata quale frutto di “errore scusabile” (cfr., Cassazione civile sez. II - 17/05/2018, n. 12110 “L'errore di diritto sulla liceità della condotta può rilevare in termini di esclusione della responsabilità amministrativa […], solo quando esso risulti inevitabile, occorrendo a tal fine, da un lato, che sussistano elementi positivi, estranei all'autore dell'infrazione, che siano idonei ad ingenerare in lui la convinzione della liceità della sua condotta e, dall'altro, che l'autore dell'infrazione abbia fatto tutto il possibile per osservare la legge, onde nessun rimprovero possa essergli mosso, neppure sotto il profilo della negligenza omissiva, gravando sull'autore dell'infrazione l'onere della prova della

sussistenza dei suddetti elementi, necessari per poter ritenere la sua buona fede"), atteso che, come peraltro noto alla stessa Azienda, l'incompletezza del quadro giuridico relativo al trattamento dei dati biometrici per finalità di rilevazione delle presenze nel settore pubblico era stata rilevata dal Garante sia con i richiamati pareri sugli atti normativi che nell'ambito di un'audizione del Presidente dell'Autorità in occasione delle audizioni presso le Commissioni riunite I (Affari Costituzionali) e XI (Lavoro) della Camera dei Deputati il 6 febbraio 2019 (doc. web n. 9080870). Tali elementi consentono quindi di escludere che, nel caso di specie, possa ricorrere "l'errore di diritto sulla liceità della condotta" ai fini dell'esclusione della responsabilità amministrativa.

Ai fini dell'applicazione della sanzione è stata considerata la particolare delicatezza dei dati personali illecitamente trattati e l'elevato numero di interessati coinvolti (tutti i dipendenti dell'Azienda ossia oltre 2000 interessati).

Di contro è stato considerato che l'Azienda ha sospeso tempestivamente il trattamento relativo al riconoscimento biometrico degli interessati e che non risultano precedenti violazioni commesse dal titolare del trattamento o precedenti provvedimenti di cui all'art. 58 del Regolamento.

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria, nella misura di euro 30.000 (trentamila) per la violazione degli artt. 5, par. 1, lett. a), 6 e 9 del Regolamento.

Tenuto conto della particolare delicatezza dei dati illecitamente trattati, si ritiene altresì che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7, del Codice e art. 16 del Regolamento del Garante n. 1/2019.

Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante.

TUTTO CIÒ PREMESSO IL GARANTE

rilevata l'illiceità del trattamento effettuato dall'Azienda sanitaria provinciale di Enna per violazione degli artt. 5, par. 1, lett. a), 6 e 9 del Regolamento, nei termini di cui in motivazione, ingiunge ai sensi dell'art. 58, par. 2, lett. d), del Regolamento la cancellazione dei dati personali (modelli biometrici) dei dipendenti attualmente memorizzati all'interno dei badge in uso agli stessi, entro sessanta giorni dalla notifica del presente provvedimento e dispone di comunicare, ai sensi dell'art. 157 del Codice, entro trenta giorni dalla data di ricezione presente provvedimento, le iniziative che intende intraprendere per assicurare la cessazione del trattamento. Il mancato riscontro a una richiesta è punito con la sanzione amministrativa, ai sensi del combinato disposto di cui agli artt. 83, par. 5, del Regolamento e 166 del Codice.

ORDINA

all'Azienda sanitaria provinciale di Enna in persona del legale rappresentante pro-tempore, con sede legale in Viale A. Diaz, 7, 94100, Enna, C.F. 01151150867 ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento e 166, comma 2, del Codice, di pagare la somma di euro 30.000,00 (trentamila) 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

alla medesima Azienda di pagare la somma di euro 30.000,00 (trentamila), in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, secondo le modalità indicate in allegato, entro 30 giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

DISPONE

la pubblicazione del presente provvedimento sul sito web del Garante ai sensi dell'art. 166, comma 7, del Codice;

l'annotazione del presente provvedimento nel registro interno dell'Autorità, previsto dall'art. 57, par. 1, lett. u), del Regolamento, delle violazioni e delle misure adottate in conformità all'art. 58, par. 2, del Regolamento.

Ai sensi dell’art. 78 del Regolamento, degli artt. 152 del Codice e 10 del d.lgs. 1° settembre 2011, n. 150, 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, 14 gennaio 2021

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei