



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Ordinanza ingiunzione nei confronti di Comune di Vicchio - 15 dicembre 2022 [9852776]

[doc. web n. 9852776]

Ordinanza ingiunzione nei confronti di Comune di Vicchio - 15 dicembre 2022

Registro dei provvedimenti
n. 422 del 15 dicembre 2022

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, 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.

A seguito di specifica segnalazione è stata avviata un'istruttoria con riferimento al trattamento di dati personali dei dipendenti effettuato da parte del Comune di Vicchio mediante un sistema utilizzato per finalità di rilevazione delle presenze che consentiva il trattamento di dati biometrici.

Nel corso dell'istruttoria è emerso, infatti, che il Comune aveva installato il predetto sistema "al fine di verificare l'osservanza dell'orario di lavoro" da parte del personale dipendente in servizio presso gli uffici comunali.

2. L'attività istruttoria.

In riscontro alle richieste di informazioni dell'Ufficio il Comune, con nota del XX (prot. n.XX), ha dichiarato che:

"in data XX, in ossequio a quanto previsto dalle disposizioni di cui alla Legge n. 56 del 2019, c.d. Legge Concretezza, il Comune, al fine di verificare l'osservanza dell'orario di lavoro, ha introdotto sistemi di verifica biometrica dell'identità dei dipendenti e, precisamente, ha installato due dispositivi di rilevazione delle presenze, forniti dalla società Halley Informatica, localizzati all'ingresso del Palazzo comunale e presso il cantiere comunale";

"il funzionamento dei sistemi di riconoscimento biometrico era così articolato:1) La fase della "registrazione" (enrolment): il lettore del terminale acquisisce l'impronta digitale e la elabora secondo un algoritmo matematico irreversibile fino ad ottenerne un modello matematico (chiamato template) che, associato al codice identificativo della persona, diviene la base dei successivi confronti o verifiche; 2) La fase della "verifica" (matching): nel momento in cui il dipendente poggia il proprio dito sopra il lettore, le caratteristiche dell'impronta digitale sono acquisite, digitalizzate, elaborate e compresse in modo identico a quello della fase di registrazione fino ad ottenerne un analogo modello matematico. Il confronto tra il modello (template acquisito in fase di registrazione) archiviato relativo al codice di riferimento ed il risultato della lettura determina, in base allo scostamento, il risultato della verifica. In tale correlazione, l'algoritmo matematico è "unidirezionale". Converte l'impronta digitale in coordinate x/y dopodiché l'algoritmo converte queste coordinate di punti in stringhe numeriche (Byte) che vengono memorizzate in un modello da utilizzare per i confronti successivi. Nel modello (template) perciò vengono memorizzati solo dei numeri di riferimento delle coordinate x/y dei punti e non la caratteristica biometrica vera e propria. Questo meccanismo rende impossibile risalire dal template all'impronta stessa, rendendo così sicura in materia di privacy, l'identità dei soggetti registrati";

"il dato biometrico era trattato e conservato in forma di modello biometrico su di un badge in possesso del singolo interessato per consentire le successive operazioni di confronto (operazioni che avvenivano con le medesime garanzie previste per la fase di enrolment)";

"il Comune ha privilegiato la conservazione dei soli modelli biometrici in dispositivi nell'esclusiva disponibilità dell'utente, evitandone l'archiviazione centralizzata in banche dati accessibili su reti anche di tipo locale";

"in ottemperanza alle disposizioni contenute nella Legge finanziaria per il 2021 e, precisamente, all'abrogazione delle disposizioni che consentivano l'introduzione di sistemi di rilevazione biometrica in ambito pubblico, in data XX ha disattivato tali sistemi e reintrodotta il badge, quale sistema di rilevazione delle presenze del personale dipendente in servizio. Il Comune ha, dunque, trattato i dati personali biometrici dei dipendenti per il periodo XX – XX, adottando, in quel contesto, tutte le misure di sicurezza per la migliore protezione e tutela dei dati personali, tanto da privilegiare, nell'ottica dei principi privacy, la conservazione dei dati su dispositivi nella disponibilità esclusiva degli interessati".

Con nota del XX, l'Ufficio, sulla base degli elementi acquisiti, ha notificato al Comune, 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 del trattamento 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 novembre 1981).

Con la nota sopra menzionata, l'Ufficio ha rilevato che il Comune ha effettuato trattamenti di dati personali biometrici dei propri dipendenti per la finalità di rilevazione delle presenze in violazione del principio di "liceità, correttezza e trasparenza" e in assenza di un idoneo presupposto di liceità, in violazione degli artt. 5, par. 1, lett. a), 6, par. 1, lett. c) e 9 par. 2, lett. b), e par. 4, del Regolamento.

Con nota del XX, il Comune ha fatto pervenire le proprie memorie precisando, tra l'altro, che:

"l'art. 2 della legge n. 56 del 2019, stante la sua formulazione, imponeva alle Amministrazioni pubbliche l'obbligo di sostituire i previgenti sistemi di rilevazione automatica delle presenze con "sistemi di verifica biometrica dell'identità nel rispetto dei principi di proporzionalità, non eccedenza e gradualità sanciti dall'art. 5 par. 1 lett. c) del Regolamento (UE)";

"con provvedimento del 12 novembre 2014, n. 513, rubricato "Provvedimento generale prescrittivo in tema di biometria" il Garante per la Protezione dei dati Personali definiva "un quadro unitario di misure e accorgimenti di carattere tecnico, organizzativo e procedurale per accrescere i livelli di sicurezza dei trattamenti biometrici e per conformarli alla vigente disciplina della protezione dei dati personali" (cfr. Premesse all'allegato A) provvedimento del 12.11.2014, n. 513 GPDP)";

"merita rilevare come il parere rilasciato dal Garante sullo schema di DPCM di cui all'art. 2 L. 56/2019, indica l'opportunità di integrare il testo regolamentare con le prescrizioni di cui al provvedimento n. 513/2014 innanzi richiamato al fine di adempiere all'obbligo normativo disposto dall'art. 2 della L. 56/2019 [...]";

"il sistema di rilevamento delle presenze adottato dal Comune prevedeva una fase di registrazione c.d. enrolment entro cui il lettore del terminale leggeva l'impronta digitale e la rielaborava, attraverso un algoritmo matematico irreversibile, in un modello matematico crittografato costituente la base per i successivi confronti e verifiche; nella successiva fase di verifica, cd. Matching, le caratteristiche dell'impronta digitale venivano acquisite, digitalizzate ed elaborate nella medesima modalità della fase di registrazione fino ad ottenere lo stesso modello matematico. Il confronto tra il modello archiviato relativo al codice di riferimento ed il risultato della lettura determinava il risultato della verifica. L'algoritmo matematico utilizzato non consentiva di memorizzare le caratteristiche somatiche del dato biometrico. Inoltre, il sistema così come realizzato non consentiva di risalire dal modello matematico generato dall'impronta digitale";

"come indicato nella informativa trasmessa ai dipendenti del Comune nell'XX, dopo la registrazione, il template viene memorizzato per poter essere in seguito confrontato, come spiegato in precedenza. Nel nostro caso il template non è memorizzato direttamente nella memoria del dispositivo lettore, ma su un badge da consegnare al dipendente che resta personalmente responsabile della conservazione. I dati che vengono archiviati sono i seguenti: a) Il codice utente: trattasi di un semplice codice di riferimento; b) Il modello template: trattasi di un puro numero che viene memorizzato sul badge in dotazione al dipendente. I confronti tra quello memorizzato e quello generato al momento della registrazione vengono eseguiti sempre a livello locale senza lasciarli poi memorizzati sul terminale. Questa modalità garantisce ulteriormente il dipendente sulla riservatezza del dato, poiché il template è memorizzato solo sul badge dato in dotazione. c) L'elenco degli eventi: trattasi della data, ora, codice utente, indirizzo del terminale ed eventuale codice del giustificativo. Questi sono gli unici risultati memorizzati dopo le verifiche operate dal lettore biometrico. In pratica sono dati equivalenti ai dati classici di qualsiasi terminale di rilevazione delle presenze del personale. Nel lettore biometrico del terminale NON sono quindi presenti:

a) I dati anagrafici del dipendente; b) L'immagine dell'impronta digitale del dipendente; c) Dati fisici diretti o deducibili dell'impronta digitale. La "ricostruzione" dell'impronta digitale del dipendente partendo dal template non è possibile, nemmeno conoscendo il codice dell'algoritmo di elaborazione per definizione stessa di algoritmo matematico irreversibile";

"il Comune nell'utilizzare il sistema di rilevamento delle presenze innanzi descritto si [è] conformato alle prescrizioni dettate dallo stesso Garante con provvedimento n. 513/2014 e dell'all. A. [...e non ha] posto in essere una condotta concretamente offensiva degli interessi sottesi alle norme del Regolamento UE";

"l'esimente della buona fede, intesa come errore sulla liceità del fatto, applicabile anche in tema di illecito amministrativo disciplinato dalla l. 689/1981, assume rilievo in presenza di elementi positivi idonei ad ingenerare nell'autore della violazione il convincimento della liceità del suo operato (Corte appello sez. I - Milano, 06/05/2021, n. 369). In altri termini "In tema di sanzioni amministrative, ai sensi della legge n. 689 del 1981, articolo 3, per le violazioni colpite da sanzione amministrativa è necessaria e al tempo stesso sufficiente la coscienza e volontà della condotta attiva o omissiva, senza che occorra la concreta dimostrazione del dolo o della colpa, giacché la norma pone una presunzione di colpa in ordine al fatto vietato a carico di colui che lo abbia commesso, riservando poi a questi l'onere di provare di aver agito senza colpa. Ne deriva che l'esimente della buona fede, applicabile anche all'illecito amministrativo disciplinato dalla legge n. 689/1981, rileva come causa di esclusione della responsabilità amministrativa - al pari di quanto avviene per la responsabilità penale, in materia di contravvenzioni - solo quando sussistano elementi positivi idonei a ingenerare nell'autore della violazione il convincimento della liceità della sua condotta e risulti che il trasgressore abbia fatto tutto quanto possibile per conformarsi al precetto di legge, onde nessun rimprovero possa essergli mosso (Cass. civile sez. II - 23/02/2021, n. 4830)";

"a norma di cui all'art. 2 legge n.56/2019 imponeva alle Amministrazioni pubbliche l'obbligo di sostituire i previgenti sistemi di rilevazione automatica delle presenze con "sistemi di verifica biometrica dell'identità [...] Allo stesso tempo, tuttavia, in modo contraddittorio, non veniva emanato il decreto attuativo previsto dalla seconda parte del medesimo articolo, creando, per l'effetto, nei destinatari del precetto legislativo un inevitabile disorientamento sulla corretta condotta da assumere";

"l'Amministrazione Comunale al fine, comunque, di conformarsi a quanto prescritto dalla prima parte della disposizione legislativa richiamata ed al contempo di rispettare i principi di cui all'art. 5 del Regolamento UE, ha adottato il sistema biometrico di rilevamento delle presenze innanzi descritto, conformemente al provvedimento del Garante n. 513/2014 [...] valutando il rilievo biometrico delle presenze adottato come "autorizzato" dallo ordinamento italiano, essendo prescritto dalla prima parte dell'art. 2 della L. n. 56/2019 e, altresì, realizzato in modo tale da garantire i diritti fondamentali degli interessati; così da essere rispettoso del provvedimento del Garante n. 513/2014";

"Il complesso quadro normativo innanzi descritto ha, pertanto, ingenerato nell'Amministrazione il convincimento della liceità della sua condotta, risultando per l'effetto il Comune non meritevole dell'applicazione di un trattamento sanzionatori".

In data XX si è, inoltre, svolta l'audizione richiesta dal Comune, ai sensi dell'art. 166, comma 6, del Codice, in occasione della quale lo stesso ha confermato quanto già dichiarato in sede di memorie difensive, precisando, tra l'altro, che:

"il Comune di Vicchio è un ente di piccole dimensioni, con soli cinquanta dipendenti;

"il Comune ha fatto riferimento al provvedimento generale del Garante del 2014 in materia di

biometria al fine di assicurare il rispetto dell'art. 5 del Regolamento (UE) 2016/679, dotandosi di uno strumento di rilevazione delle presenze conforme alle prescrizioni del Garante, non andando a ledere gli interessi che l'art. 2 della l. 56/2019 intendeva tutelare”;

“il sistema è stato utilizzato fino all'XX e, pertanto, per soli undici giorni dopo l'abrogazione dell'art. 2 della l. 56/2019, ovvero per un tempo del tutto ragionevole per consentire all'Ente di ripristinare gli ordinari sistemi di rilevazione delle presenze”;

“il sistema di rilevazione biometrica è stato in ogni caso impostato nella massima sicurezza e nel pieno rispetto dei diritti degli interessati, essendo il trattamento conforme alle prescrizioni a suo tempo impartite dal Garante con il predetto provvedimento del 2014 in materia di biometria. Era stata, peraltro, fornita ai lavoratori una specifica informativa sul trattamento dei dati personali”;

“tutti i dati biometrici (che si riferivano ad un numero di interessati comunque non superiore a cinquanta, tenuto conto del periodo emergenziale legato alla pandemia da SARS-CoV-2) sono stati in ogni caso definitivamente cancellati”.

3. Esito dell'attività istruttoria. La normativa applicabile.

La disciplina di protezione dei dati personali prevede che il datore di lavoro può trattare i dati personali dei dipendenti, anche relativi a categorie particolari (cfr. art. 9, par. 1 del Regolamento), se il trattamento è necessario, in generale, per adempiere a specifici obblighi o compiti previsti dalle norme nazionali di settore e, in generale, per la gestione del rapporto di lavoro con l'interessato e per adempiere a specifici obblighi o compiti previsti dalla legge o dal diritto dell'Unione o degli Stati membri (artt. 6, par. 1, lett. c), 9, parr. 2, lett. b), e 4, e art. 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” (art. 6, parr. 1, lett. e), 2 e 3, e art. 9, par. 2, lett. g), del Regolamento; art. 2-ter del Codice, nel testo antecedente alle modifiche apportate dal d.l. 8 ottobre 2021, n. 139).

Con specifico riguardo ai dati biometrici, ossia “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, par. 1, n. 14) del Regolamento), occorre sottolineare che, come ormai noto, in ragione della loro delicatezza - derivante dalla stretta (e stabile) relazione con l'individuo e la sua identità - essi sono ricompresi tra le categorie “particolari” di dati personali (art. 9 del Regolamento).

In tale quadro, il trattamento di dati biometrici - di regola vietato- è consentito soltanto al ricorrere di una delle condizioni indicate dal par. 2 dell'art. 9 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 3 fondamentali e gli interessi dell'interessato” (v. pure, art. 88, par. 1, del Regolamento e cons. 51-53).

Il quadro normativo vigente prevede altresì che il trattamento di dati biometrici, per poter essere lecitamente posto in essere, avvenga nel rispetto di “ulteriori condizioni, comprese limitazioni” (cfr. 9, par. 4 del Regolamento) che, nell'ordinamento nazionale, consistono nella “conformità alle misure di garanzia disposte dal Garante”, ai sensi dell'art. 2-septies del Codice.

Il datore di lavoro, titolare del trattamento, è, in ogni caso, tenuto a rispettare i principi di “liceità,

correttezza e trasparenza”, “limitazione della finalità”, “minimizzazione dei dati”, “esattezza”, nonché “integrità e riservatezza” e “responsabilizzazione” (art. 5 del Regolamento).

3.1 Il trattamento dei dati biometrici dei dipendenti per finalità di rilevazione delle presenze

La finalità di rilevazione delle presenze in servizio dei dipendenti, funzionale all’attestazione dell’osservanza dell’orario di lavoro e 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) - 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).

In merito alla compatibilità rispetto alla disciplina di protezione dei dati personali del perseguimento di tale finalità mediante il trattamento di dati biometrici, occorre ricordare che fin dal 2007, nel quadro normativo previgente che non includeva tali categorie di dati tra quelli sensibili, 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 dichiarando l’illiceità dei trattamenti effettuati nel contesto lavorativo a fronte di generiche esigenze di prevenzione di eventuali comportamenti scorretti o di utilizzo distorto degli strumenti di rilevazione delle presenze d’uso comune, quali i badge (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; 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).

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 personnels”).

Nel quadro delineato dal Regolamento, come già anticipato (cfr. par. 3), il trattamento di dati biometrici richiede oggi 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).

Il rafforzamento delle tutele dei dati biometrici previste dal Regolamento e dal Codice, mediante l’inclusione degli stessi nelle categorie di dati particolari e, al pari dei dati sulla salute e genetici, tra quelle assistite da un più elevato livello di garanzie, ha infatti riguardato anzitutto i presupposti giuridici che giustificano i trattamenti di tali categorie di dati (cfr. provv. 14 gennaio 2021, doc. web n.9542071, n. 16, doc. web n.9542071; v. anche, più in generale, con riguardo ad un diverso contesto, provv. 16 settembre 2021, n. 317, doc web n. 9703988).

In tale contesto, quindi, il trattamento di dati biometrici può essere lecitamente effettuato solo ove

lo stesso trovi il proprio fondamento in una disposizione normativa che abbia le caratteristiche richieste dalla disciplina di protezione dei dati 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, par. 2 e 3 del Regolamento). Ciò in quanto, il diritto nazionale, per poter essere considerato una valida condizione di liceità del trattamento, deve, tra l'altro, "persegui[re] un obiettivo di interesse pubblico ed [essere] proporzionato all'obiettivo legittimo perseguito" (art. 6, par. 3, lett. b), del Regolamento).

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. 30 marzo 2001, n. 165, 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 l. 22 maggio 2017, n. 81 - "introducono sistemi di identificazione biometrica e di videosorveglianza in sostituzione dei diversi sistemi di rilevazione automatica attualmente in uso".

Tale generica previsione stabiliva 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 – dovessero essere individuate con d.P.C.M., su proposta del Ministro per la Pubblica Amministrazione, 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 154 del Codice), il Garante aveva, a suo tempo, segnalato al legislatore nazionale le rilevanti criticità della proposta normativa 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).

Come ribadito dal Garante anche successivamente, nel corso dell'audizione in Parlamento in relazione a tale intervento normativo, il rispetto del principio di proporzionalità deve essere, infatti, assicurato anche nell'ambito del bilanciamento tra interessi pubblici diversi e diritti fondamentali operato dal potere legislativo degli Stati membri. Anche in ragione della stretta correlazione tra l'art. 8 della Convenzione Europea dei Diritti dell'Uomo e gli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, prevista dall'art. 52 della Carta medesima, quando una misura legislativa, che deve comunque rispondere a finalità di interesse generale, sia interferente o limitativa di un diritto tutelato dall'ordinamento comunitario, occorre valutare se essa rispetti il "contenuto essenziale dei diritti" e rappresenti la "misura meno restrittiva" per raggiungere lo scopo legittimo che si intende perseguire con "minor sacrificio possibile degli interessi coinvolti" nel rispetto del principio di proporzionalità (cfr., audizione del Presidente dell'Autorità presso le Commissioni riunite I e XI, Affari Costituzionali e Lavoro, della Camera dei Deputati il 6 febbraio 2019, doc. web n. 9080870).

Alla luce di tale quadro, le previsioni normative che introducono/autorizzano un trattamento di dati personali possono determinare compressioni del diritto alla protezione dei dati personali nei limiti dello stretto necessario (devono essere "necessarie" all'interesse meritevole di tutela che si intende perseguire in presenza di una "pressante esigenza sociale") e devono rispondere effettivamente a finalità di interesse generale nel rispetto del principio di proporzionalità, graduando le forme di intervento e prediligendo quelle che, nel consentire l'effettività degli obiettivi da perseguire, determinino invasioni meno gravi nella "vita privata" degli interessati (v. la copiosa

giurisprudenza della Corte Europea dei diritti dell'uomo, causa c-524/06-Huber/Bundesrepublik Deutschland del 16/12/2008, nonché della Corte di giustizia dell'Unione europea, Grande Sezione, 8 aprile 2014, Cause riunite C-293/12 e C-594/12; sentenza 20 maggio 2003, C-465/00, C-138/01 e C-139/01, riunite; sentenza 9 novembre 2010, C-92/09 e C-93/09, riunite).

Come messo in luce anche dalla giurisprudenza costituzionale, nel bilanciamento di valori concorrenti, ancorché di rilevanza costituzionale, occorre verificare che la soluzione prescelta dal legislatore, tra le misure astrattamente possibili, sia la più appropriata al conseguimento degli obiettivi e sia, al contempo, quella meno restrittiva dei diritti, pena la irragionevolezza e sproporzione della misura legislativa (cfr. sent. della Corte costituzionale n. 20 del 23 gennaio 2019, punto n. 5).

Confermando quanto già rilevato nel corso delle audizioni dinanzi alle Commissioni parlamentari competenti, il Garante ha, quindi, ribadito, anche in relazione allo schema di d.P.C.M. che avrebbe dovuto contenere le relative disposizioni di attuazione, poi ritirato in conseguenza dei rilievi dell'Autorità e 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” (cfr. parere n. 167 del 19 settembre 2019, 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 poi abrogate dalla l. 30 dicembre 2020, n. 178 (c.d. legge di bilancio 2021, art. 1, comma 958).

Per tali ragioni, come ribadito dall'Autorità in decisioni su singoli casi nei confronti di altri titolari del trattamento in ambito pubblico adottando i conseguenti provvedimenti correttivi e sanzionatori, in assenza di proporzionate misure legislative e di specifiche garanzie per gli interessati, il trattamento dei dati biometrici per la predetta finalità di rilevazione delle presenze dei dipendenti non poteva e non può essere effettuato (cfr., da ultimo, provv. 14 gennaio 2021, n. 16, doc. web n. 9542071, cit.; v. le analoghe considerazioni con riguardo al contesto privato, provv. n. 369 del 10 novembre 2022, in corso di pubblicazione).

Nel corso dell'istruttoria il Comune ha fatto presente che, stante la mancata adozione delle disposizioni di attuazione della citata legge, avrebbe effettuato alcune scelte e adottato misure tecniche al fine di rispettare il quadro normativo di protezione dei dati e il provvedimento generale prescrittivo in tema di biometria (provv. del 12 novembre 2014, n. 513 doc web n. 3556992. Al riguardo il Comune ha dichiarato che “il template [... biometrico non era] memorizzato direttamente nella memoria del dispositivo lettore, ma su un badge da consegnare al dipendente che resta personalmente responsabile della conservazione”, garantendo “ulteriormente il dipendente sulla riservatezza del dato, poiché il template è memorizzato solo sul badge dato in dotazione”.

Tali circostanze non sono, tuttavia, sufficienti ad escludere la responsabilità del titolare nel caso di specie.

Nel premettere che il richiamato provvedimento generale non contempla l'impiego dei dati biometrici per la specifica finalità di rilevazione delle presenze - avendo invece ad oggetto i casi di “utilizzo di dispositivi e tecnologie per la raccolta e il trattamento di dati biometrici [...] per l'accertamento dell'identità personale nell'ambito dell'erogazione di servizi della società dell'informazione e dell'accesso a banche dati informatizzate, per il controllo degli accessi a locali e aree, per l'attivazione di dispositivi elettromeccanici ed elettronici, anche di uso personale, o di

macchinari, nonché per la sottoscrizione di documenti informatici” (cfr. premessa, provv. n. 513 cit.) – si osserva quanto segue.

Le misure adottate e descritte dal Comune rispondono a una scelta progettuale del titolare che, al momento di determinare i mezzi del trattamento, adotta le misure tecniche e organizzative - in attuazione dei principi di responsabilizzazione, minimizzazione e protezione dati fin dalla progettazione e per impostazione predefinita (cfr. artt. 5, par. 1, lett. c) e par. 2, 24 e 25 del Regolamento) - restando però, in ogni caso, necessaria la preliminare verifica in ordine alla ricorrenza (o meno) dei presupposti di liceità per trattare i dati biometrici dei dipendenti per la specifica finalità considerata (art. 9 del Regolamento). Peraltro, anche nel previgente quadro normativo, allorquando i dati biometrici non erano considerati, diversamente da oggi, dati “sensibili”, la modalità di memorizzazione/conservazione dei dati biometrici adottata in concreto dal titolare del trattamento era stata espressamente indicata dal Garante tra le misure e gli accorgimenti di carattere tecnico per garantire la proporzionalità e la sicurezza del trattamento ma da mettere in campo sempre comunque previa verifica della sussistenza 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 doc web n. 3556992).

Né, del resto, come messo in evidenza nel parere che il Garante ha reso sul citato schema di d.P.C.M. (parere noto al titolare del trattamento per averlo espressamente richiamato nel corso dell’istruttoria) “il vizio che connota in radice la norma” non potrebbe essere “sanato riferendo il rispetto del canone di proporzionalità alle specifiche modalità attuative di tale obbligo di rilevazione biometrica (modulando diversamente, ad esempio, le tipologie di dati utilizzati o il termine di conservazione), che potrebbe soltanto ridurre l’impatto sul diritto alla protezione dei dati degli interessati”. In quella occasione il Garante ha, altresì, precisato che “l’incompatibilità di tale previsione con i principi di proporzionalità, non eccedenza, minimizzazione risiede infatti nell’an prima che nel quomodo del trattamento [ossia] nella sua configurazione come astrattamente obbligatoria a prescindere da qualsiasi esigenza concreta e specifica in tal senso”, concludendo che “le criticità rilevate a proposito dell’articolo 2 della legge n. 56 del 2019 che [...] si estendono quindi, inevitabilmente, anche allo schema di regolamento chiamato ad attuarne il disposto” (cfr., parere n. 167 del 19 settembre 2019, doc. web n. 9147290, cit.).

Alla luce delle considerazioni che precedono, si ritiene che il Comune abbia effettuato, dal XX all’XX, il trattamento dei dati biometrici dei propri dipendenti per finalità di rilevazione delle presenze, in assenza di un’idonea base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6 e 9, par. 2, lett. b), e par. 4, del Regolamento.

Contrariamente a quanto ritenuto dal titolare del trattamento, la condotta non può essere considerata inoltre 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”).

Con riguardo al caso di specie, infatti, l’incompletezza del quadro giuridico relativo al trattamento dei dati biometrici per finalità di rilevazione delle presenze nel settore pubblico - in aggiunta alle criticità sotto il profilo della proporzionalità dell’intervento normativo - era stata rilevata dal Garante sia con i richiamati pareri sugli atti normativi che 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 circostanze e la mancata adozione di norme di attuazione risultano ben note al titolare del trattamento, come peraltro evidenziato dallo stesso a giustificazione delle proprie scelte sotto il profilo tecnico, con ciò dovendosi escludere che, nel caso di specie, possa ricorrere "l'errore di diritto sulla liceità della condotta" ai fini dell'esclusione della responsabilità amministrativa.

Né può essere accolta la tesi secondo cui il Comune avrebbe agito credendo di essere obbligato ad installare il predetto sistema in quanto alcuna conseguenza era stata prevista per le amministrazioni in caso di mancata attivazione dei predetti sistemi di rilevazione delle presenze e come confermato dal fatto che il Comune si è dotato del sistema in questione in data XX, ben oltre un anno dopo la legge n. 56/2019. Al riguardo occorre infine considerare che l'installazione del sistema è avvenuta in un periodo, il 2020, caratterizzato dall'emergenza epidemiologica da Sars-Cov-2, allorquando era stato disposto dalle norme emergenziali l'ampio ricorso al lavoro agile quale misura di contenimento della circolazione del virus negli ambienti di lavoro, specialmente pubblici, ad eccezione delle attività che per propria natura non potessero essere svolte in modalità agile (cfr., art. 87, d.l. del 17 marzo 2020 n. 18 e art.1, lett. d) del d.P.C.M. del 22 marzo 2020, che prevedevano lo svolgimento in modalità agile quale "modalità ordinaria di svolgimento della prestazione lavorativa nelle pubbliche amministrazioni" e, successivamente, art. 2 d.l. 30 del 13 marzo 2021 nonché art. 6, d.P.C.M 2 marzo 2021, in relazione al fatto che nelle pubbliche amministrazioni dovesse essere assicurato "lo svolgimento del lavoro agile nella percentuale più elevata possibile").

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 e indicative della piena collaborazione del titolare del trattamento al fine di attenuare i rischi del trattamento, rispetto alla situazione presente all'atto dell'avvio dell'istruttoria, non consentono tuttavia di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano quindi 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 in quanto avvenuto in violazione degli artt. artt. 5, 6 nonché art. 9, par. 2, lett. b) e par. 4 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 e dell'art. 166, comma 2, del Codice.

In tale quadro, considerando che la condotta ha esaurito i suoi effetti, non ricorrono invece i presupposti per l'adozione di misure correttive, di cui all'art. 58, par. 2, del Regolamento.

5. 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.

Ai fini dell'applicazione della sanzione è stata considerata la particolare delicatezza dei dati personali trattati, di natura biometrica, rispetto ai quali il quadro normativo in materia di protezione dei dati personali prevede il livello più alto di tutela; il numero degli interessati coinvolti, ossia i cinquanta dipendenti del Comune, nonché l'arco temporale per il quale il trattamento si è protratto (dal XX all'XX) e il contesto storico di attivazione del sistema, stante l'emergenza epidemiologica e l'ampio e generalizzato ricorso al lavoro agile nelle amministrazioni pubbliche.

Di contro è stato considerato che il Comune ha sospeso il trattamento relativo al riconoscimento biometrico degli interessati, ha fornito un'adeguata collaborazione nel corso dell'istruttoria provvedendo a cancellare definitivamente tutti i dati raccolti e una attiva collaborazione con il Garante nel corso dell'attività istruttoria; da ultimo l'ambiguità del dato normativo di rango primario che può aver indotto in errore scusabile il Comune medesimo. 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 8.000,00 (ottomila) per la violazione degli artt. 5, 6 nonché art. 9, par. 2 e par. 4 del Regolamento

Tenuto conto della particolare natura dei dati personali oggetto di trattamento e dei connessi rischi per gli interessati nel contesto lavorativo, 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 dall'art. 16 del Regolamento del Garante n. 1/2019.

Si ritiene, 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

rileva l'illiceità del trattamento effettuato dal Comune di Vicchio per la violazione degli artt. 5, 6 nonché art. 9, par. 2, e par. 4, del Regolamento, nei termini di cui in motivazione;

ORDINA

al Comune di Vicchio, in persona del legale rappresentante pro-tempore, con sede legale in Via Garibaldi n. 1, 50039 Vicchio (Firenze), C.F. n. 83002370480 - Partita IVA 01443650484 ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento, di pagare la somma di euro 8.000,00 (ottomila) 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 trenta giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

al Comune di Vicchio di pagare la somma di euro 8.000,00 (ottomila) in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, secondo le modalità indicate in allegato, entro trenta 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, 15 dicembre 2022

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei