Registro dei provvedimenti
n. 231 del'1° giugno 2023

## 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, componente e il cons. Fabio Mattei, segretario generale;

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

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

VISTA la segnalazione presentata nei confronti di Ew Business Machines S.p.A.;

ESAMINATA la documentazione in atti;

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

RELATORE la prof.ssa Ginevra Cerrina Feroni;

## PREMESSO

### 1. La segnalazione nei confronti della Società e l'esito degli accertamenti ispettivi.

Con segnalazione presentata all'Autorità il 22 novembre 2019, è stato lamentato che Ew Business Machines S.p.A. (di seguito, la Società) avrebbe utilizzato, presso la propria sede, un sistema di

videosorveglianza, con attiva la funzione di registrazione e in assenza di informativa, un sistema di rilevazione delle impronte digitali dei dipendenti e un sistema di rilevazione della posizione geografica dei dipendenti tramite applicativo installato sui cellulari degli stessi.

Considerata la natura delle violazioni lamentate, l'Ufficio ha delegato al Nucleo speciale tutela privacy e frodi tecnologiche della guardia di finanza lo svolgimento dell'accertamento ispettivo che è stato effettuato, in data 21 e 22 giugno 2021, presso la sede legale della Società.

In occasione dell'accertamento ispettivo la Società, attraverso il proprio legale rappresentante, ha rappresentato (v. verbale di operazioni compiute del 21 e 22 giugno 2021) che "a seguito di un accesso abusivo a scopo di furto subito a fine settembre 2019 si è deciso di sostituire il sistema di allarme, in quanto quello in uso non aveva rilevato l'effrazione avvenuta e con attivazione e disattivazione a mezzo impronta digitale; nonché di installare una telecamera interna, in corrispondenza della reception, in modo da poter rilevare eventuali accessi indesiderati nelle ore di chiusura degli uffici e poter, quindi, intervenire; […] il sistema di allarme è stato installato anche presso il magazzino, sito al piano -1 di questa scala, e presso i locali siti al 1° piano […], la telecamera, invece, è stata installata presso la reception in quanto, quest'ultima, è l'ambiente di raccordo con le altre stanze di questa unità immobiliare; relativamente alla posizione geografica dei tecnici, posso ipotizzare che si faccia riferimento agli smartphone in dotazione degli stessi sui quali è installata l'app […] di gestione delle chiamate e degli interventi controllati centralmente".

Durante il suddetto accertamento è emerso che:

- "la parte, appena venuta a conoscenza del motivo della visita, ha mostrato l'app di gestione della […] telecamera, dalla quale si è potuto constatare che la stessa era disattiva";

- con riferimento al sistema di videosorveglianza era "presente una sola telecamera […], orientata verso l'area antistante il desk della reception, collegata alla rete elettrica; non è presente alcun cartello informativo, né esterno né interno, circa la presenza di detta telecamera, e non sono presenti altre telecamere presso i locali delle altre unità immobiliari in uso alla società";

- con riferimento all'impianto d'allarme "presso la reception sono installati la centrale e un rilevatore di impronte digitali, mentre, presso le altre due unità immobiliari, sono installati altri due rilevatori di impronte, uno per ogni unità immobiliare";

- relativamente alla "gestione della telecamera in argomento, la parte ha mostrato le funzionalità della relativa app installata sul proprio smartphone personale. […] da quanto mostrato e da quanto dichiarato è emerso che: - l'app utilizzata è denominata "Nest"; - l'app rileva anche immagini relative all'abitazione della parte; - la videocamera [presente presso la sede della Società] risulta spenta e attivabile tramite apposito pulsante; - l'account è associato al [rappresentante legale della Società]; - il sistema di videosorveglianza rilevato dall'app si compone di 5 telecamere domestiche e una installata presso l'ufficio"; "tra le impostazioni relative alla telecamera installata presso l'ufficio risulta attiva la funzione "registrazione video" al cui riguardo la parte ha fatto presente che il sistema effettua la registrazione nel momento in cui la telecamera viene accesa e al verificarsi di eventi (movimento e/o suoni); la telecamera consente di registrare anche suoni ed è dotata di speaker per la riproduzione di audio effettuati tramite la funzione "microfono" dell'app; - la sezione relativa alla videocamera offline è riferita alla telecamera installata presso il salotto dell'abitazione della parte; - al fine di constatare i tempi di conservazione delle immagini registrate, la parte ha mostrato lo storico delle registrazioni della telecamera relativa all'ambiente "terrazzo" (puntata sulla piscina), dal quale risulta la conservazione di 33 eventi nel periodo che va dal 2

maggio 2021 ad oggi; - attivando tramite la suddetta funzione la telecamera installata presso la reception, l'app ha restituito l'immagine live della stessa, riprendendo l'operatrice di servizio al desk, quest'ultima inquadrata di spalle"; "dalla funzione cronologia video, relativa alla telecamera "ufficio", non sono risultati eventi salvati dal 22 maggio 2021 ad oggi, ad esclusione di quello in corso; - la telecamera è impostata per segnalare notifiche in merito a persone e non all'eventuale rilevamento di suoni/rumori"; "l'accesso al sistema è consentito a n. 4 account, dei quali uno risulta intestato alla moglie [del rappresentante legale della Società] in qualità di "proprietario" dell'abbonamento, uno [al rappresentante legale della Società] e due ai rispettivi figli".

La Società attraverso il rappresentante legale ha, inoltre, dichiarato che:

- "la telecamera "ufficio" è stata acquistata in un secondo momento rispetto a quelle installate presso la mia abitazione e per praticità di gestione è stata aggiunta all'account […]: la stessa telecamera è sempre spenta ed è stata acquistata per poter essere utilizzata qualora si attivi il sistema di allarme per poter, eventualmente, visionare/registrare eventuali intrusioni in corso nonché per ammonire verbalmente, attraverso lo speaker della telecamera; ad oggi non si è verificato nessun episodio tale da richiedere l'utilizzo della telecamera";

- "titolare del trattamento dei dati personali effettuato tramite la videocamera "ufficio" […] è la società, nata nel 2008 come Ew Business Machines s.r.l. e, dal 2015, Ew Business Machines S.p.A. […]; considerato il non utilizzo della telecamera in parola se non a seguito di attivazione del sistema di allarme, non si è ritenuto di dover apporre alcun cartello informativo all'ingresso o nelle adiacenze della stessa telecamera, anche perché raramente i nostri clienti vengono in sede […]; per quanto riguarda i dipendenti, tengo ad evidenziare che il rapporto tra la società e gli stessi si svolge in un clima familiare

risalente nel tempo, tale da informare esclusivamente a voce circa le finalità e l'utilizzo della telecamera";

- "non c'è alcun accordo sindacale in quanto non ci sono rappresentanze in azienda né l'autorizzazione preventiva della Direzione Territoriale del Lavoro circa l'installazione e l'utilizzo della telecamera in parola".

Con riferimento al sistema di rilevazione geografica dei tecnici - applicativo "eWBM AT"- è stato dichiarato che "l'app si interfaccia col sistema gestionale aziendale […], dal quale, a mezzo di web service dedicato, riceve informazioni circa gli interventi da assegnare al personale tecnico munito dell'app […]; l'esito dell'intervento, invece, non viene comunicato direttamente dall'app al gestionale bensì mediante email generata automaticamente dalla procedura, l'esito in parola viene comunicato al cliente, al gestionale […] nonché al tecnico operante; sia il database del gestionale che quello su cui si appoggia l'app "eWBM AT" sono ubicati all'interno dell'armadio server di questa sede".

L'operatore incaricato della gestione delle chiamate e degli interventi ha mostrato le funzionalità del gestionale aziendale, con particolare riferimento alla formulazione di una richiesta di intervento, da cui è emerso che "il gestionale non riporta alcuna informazione circa la posizione geografica dei tecnici a cui viene assegnato l'intervento".

È stato, inoltre, verificato che, nella stampa di una e-mail relativa a un intervento chiuso, fornita dall'operatore, non sono presenti "riferimenti relativi alla posizione geografica del tecnico". Sono state acquisite evidenze circa "il primo record di funzionamento dell'app, risalente all'anno 2012, il primo record di acquisizione della posizione geografica, risalente all'anno 2014, stralcio del codice sorgente dell'app relativo alle funzioni di rilevazione della posizione geografica e identificativo dei tecnici interessati".

È stato, inoltre, dichiarato dalla Società che l'applicativo "non è commerciabile, ma è ad uso esclusivo interno" e che "la rilevazione della posizione geografica è stata implementata esclusivamente per convalidare che la chiusura dell'intervento tecnico avvenisse presso il cliente".

È stato rappresentato inoltre che è possibile l'implementazione dell'applicativo con ulteriori funzioni di rilevazione della posizione geografica, con frequenza maggiore e in momenti diversi da quello della chiusura dell'intervento tecnico, previa modifica del codice sorgente dell'applicativo.

Con riferimento al sistema di rilevazione delle impronte digitali, la Società ha dichiarato che "il sistema di allarme si compone di una centrale e tre rilevatori di impronte utilizzati, esclusivamente, per attivare e disattivare il predetto sistema nonché di una scheda che funge da interfaccia tra i tre rilevatori e la centrale; ogni rilevatore consente, quindi, di gestire l'allarme nell'ambiente in cui è installato; tra i dipendenti ve ne sono alcuni abilitati a più rilevatori, di cui alcuni abilitati a tutti e tre (titolare, soci, ecc.)".

La Società ha fornito copia dell'e-mail, inviata alla società Teycos s.r.l., con cui richiedeva la relazione in merito al trattamento di dati biometrici, effettuato dal sistema di allarme e del riscontro.

Durante gli accertamenti è stato effettuato l'accesso al sistema di rilevazione delle impronte digitali ed è emerso che:

- relativamente alla centrale, "nella scheda utente sono indicati nome/nome e cognome del dipendente, numero della tessera utente (codice di riconoscimento), ambiente per il quale lo stesso è abilitato all'attivazione/disattivazione dell'impianto d'allarme e, solo per i tre soci, per necessità di notifica dell'eventuale allarme scattato, anche il recapito telefonico"; "sono presenti i log riferiti all'attivazione dell'allarme, alla sua disattivazione e i log di accesso al sistema";

- con riferimento al software dei rilevatori biometrici e, in particolare, all'ultima copia di backup delle informazioni presenti sui tre rilevatori e, a seguire, previo "upload" della copia di backup aggiornata è emerso che "sono presenti 27 impronte acquisite; è presente l'elenco dei 21 soggetti abilitati (per alcuni è stata rilevata l'impronta di più dita); per ognuno dei predetti utenti risulta la data di rilevazione dell'impronta, nome/nome e cognome, ambiente per cui è abilitata, immagine con l'indicazione del/delle dito/a rilevato/e";

- con riferimento a ogni singolo rilevatore di impronte, è emerso che "ogni rilevatore conserva le informazioni relative alla rilevazione delle impronte digitali di tutti i dipendenti censiti, indipendentemente dall'ambiente al quale sono abilitati; il numero delle impronte acquisite in ognuno di essi risulta essere pari a 27 e risultano presenti le medesime informazioni, come nella copia di backup aggiornata al momento". La Società ha confermato che "ogni rilevatore conserva le informazioni di tutti gli utenti abilitati al sistema a prescindere dalle abilitazioni".

In sede di ispezione, inoltre, su richiesta dei verbalizzanti, sono stati estratti e forniti "i log di acceso al server contenente il database su cui appoggia l'app […] specificamente riferiti al periodo che va dalle ore 00:00 del 21 giugno alle ore 11:45:08 odierne. Detti log forniscono informazioni circa login e logout di tutti gli utenti a sistema con l'indicazione dell'IP di origine".

In merito al funzionamento dell'app "eWBM AT" e alle funzioni di sistema relative alla rilevazione della posizione geografica dei tecnici durante gli interventi, la Società ha provveduto a "mostrare la funzione del codice sorgente relativa alla rilevazione-tracciamento della posizione geografica dell'Iphone del tecnico al momento della chiusura della chiamata (conclusione dell'intervento); - effettuare una nuova simulazione di chiamata dal gestionale alla sua utenza e alla gestione/chiusura della stessa, previa attivazione della rilevazione della posizione geografica, impostandola in modalità "mentre usi l'app", sia dalle impostazioni

generali dell'Iphone che dalla stessa app; dalla predetta operazione è emerso che nella tabella "dbo.tab_gpstracking", utilizzata per memorizzare i tracciamenti gps provenienti dagli utenti dell'app, è risultata tracciata in modo continuo la posizione dell'Iphone d[el'amministratore di sistema] (espressa in latitudine e longitudine), dall'accesso all'app alla chiusura della simulazione di chiamata, ad esclusione del periodo in cui l'app non è stata utilizzata; allo stesso modo, è risultata tracciata in modo continuo la posizione dell'iphone in dotazione ad un altro tecnico […], selezionato a campione, dalle ore 8:21:40 odierne al momento della verifica (12:56:49)".

La Società ha, inoltre, dichiarato che:

- con specifico riferimento al trattamento del dato relativo alla posizione geografica, "il sistema traccia la posizione geografica dell'iPhone, previo accesso all'app, e a condizione che la stessa sia attiva; quindi in caso di app in background piuttosto che con smartphone in standby il sistema non effettua il tracciamento";

- con riferimento al sistema di allarme associato alla rilevazione delle impronte digitali, "in considerazione della relazione che ci è stata fornita dalla società Teycos s.r.l. e, quindi, da quanto riportato nella stessa con la frase "nessuna impronta in chiaro viene memorizzata nel terminale né tantomeno nella centrale di gestione", non si è ritenuto di effettuare alcun trattamento di dati personali; pertanto i nostri dipendenti sono stati informati verbalmente circa la finalità e l'utilizzo del suddetto sistema, con l'indicazione specifica che nessun dato sarebbe rimasto in memoria; anche per questo non è stato inserito nel registro dei trattamenti dei dati personali";

- con riferimento ai trattamenti di dati personali relativi alla posizione geografica dei dipendenti, "i trattamenti di dati personali effettuati tramite l'app sono compresi tra quelli più generali del software di gestione [aziendale], quest'ultimo riportato nel registro dei trattamenti; per quanto concerne la specifica rilevazione della

posizione geografica, non si era a conoscenza di un tracciamento continuo durante l'uso dell'app sugli Iphone in dotazione ai tecnici, ma eravamo al corrente della sola rilevazione all'atto della chiusura della chiamata […] e che è utile alla società per far fronte ad eventuali lamentele/contestazioni da parte dei clienti circa la durata dell'intervento tecnico: per queste ragioni non si è ritenuto di dover prendere in considerazione le previsioni di cui allo statuto dei lavoratori";

- "Teycos s.r.l. non è mai stata nominata responsabile del trattamento".

In data 7 luglio 2021, la Società ha inviato documentazione integrativa evidenziando che:

- "Il [lavoratore che si occupa dello sviluppo e della manutenzione dell'app eWBm AT] è stato da noi nominato amministratore di sistema";

- "la nostra società dispone di diversi uffici a vari piani di uno stabile […] in Milano ma una sola telecamera è stata posizionata in ingresso […] con il solo scopo di individuare eventuali intrusi in orario extra-lavorativo… fortunatamente non è mai stata necessaria la sua accensione";

- "il nostro impianto di allarme (uno per piano) viene inserito o disinserito tramite lettura di impronta digitale dalla prima/ultima persona che entra/esce in/dall'ufficio… la persona non è mai la stessa, spessissimo sono i titolari stessi ad eseguire tale funzione e la nostra azienda […] non ha assolutamente accesso alle impronte digitali registrate nell'impianto (non sono nemmeno presenti le impronte di tutti i dipendenti ma solo di quelli che potrebbero avere necessità di inserire/disinserire l'impianto di allarme)";

- "la nostra app eWBM AT (interamente sviluppata internamente) ci permette di smistare le chiamate ricevute dai nostri clienti quasi in

tempo reale ai nostri tecnici che pertanto hanno la possibilità di risolvere rapidamente i guasti delle apparecchiature da noi fornite";

- "una delle tipologie dei nostri interventi è quella a pagamento (ore del tecnico presso il cliente ed eventuali km percorsi dallo stesso per recarsi all'appuntamento) … si è pertanto reso necessario il tracciamento per poter dimostrare ai clienti quanto effettivamente fatturato. […] i nostri tecnici sono consapevoli che tale tracciamento è abilitato ad app accesa (quindi quando si trovano dal cliente) ed hanno sempre e comunque la possibilità di abilitare e disabilitare tale funzione".

In data 12 luglio 2021 la Società ha inviato un'ulteriore integrazione documentale.

## 2. L'avvio del procedimento e le deduzioni della Società.

In data 29 novembre 2021, l'Ufficio ha effettuato, ai sensi dell'art. 166, comma 5, del Codice, la notificazione alla Società delle presunte violazioni del Regolamento riscontrate, con riferimento agli artt. 114 del Codice, 5, par. 1, lett. a), c), 6, 9, 13 e 88 del Regolamento.

Con memorie difensive del 23 dicembre 2021, la Società ha dichiarato che:

- "tanto dalla lettura del processo verbale che dalla notifica delle presunte violazioni emerge […] la particolarità del caso" (v. nota 23.12.2021 cit., p. 6);

- "appare evidente la intrinseca buona fede che ha caratterizzato le scelte del Titolare del trattamento, seppur non sempre allineate in termini di accountability" (v. nota cit., p. 6);

- "l'installazione della telecamera denominata "ufficio", accessibile a mezzo applicativo, è conseguita alla necessità di mettere in sicurezza il patrimonio aziendale "in seguito ad un accesso abusivo

a scopo di furto", risalente al mese di settembre 2019" (v. nota cit., p. 7);

- "dal punto di vista squisitamente normativo, pertanto, non pare revocabile in dubbio che gli scopi perseguiti dal Titolare del trattamento fossero determinati, espliciti e legittimi. Egualmente dicasi del rispetto dei principi di liceità, necessità e proporzionalità" (v. nota cit., p. 7);

- "nel commisurare la necessità di un sistema (composto, peraltro, da una sola telecamera) è stato valutato il grado di rischio presente in concreto, evitando la rilevazione di dati in aree, ovvero attività, che non sono soggette a concreti pericoli oppure per le quali non ricorre una effettiva esigenza di deterrenza. Al contrario, l'installazione è stata espressamente finalizzata alla protezione di beni aziendali, soprattutto in relazione ad episodi di furto tentato e combinata con altri idonei accorgimenti quali, per l'appunto, un rinnovato sistema di allarme abbinato a misure di protezione ed abilitazione agli ingressi" (v. nota cit., p. 7, 8);

- "il Titolare del trattamento ha peccato di ingenuità - ritenendo di aver correttamente adempiuto al proprio obbligo di trasparenza nei confronti degli interessati, mediante comunicazione orale (e pur sempre nel rispetto delle previsioni di cui all'art. 12 GDPR) - quando, invece, avrebbe dovuto predisporre una modalità di comunicazione intellegibile, trasparente e facilmente accessibile" (v. nota cit., p. 8, 9);

- "le condizioni generali vanno contestualizzate al caso di specie ed allora tre sono i rilievi che vanno tenuti in debito conto: i. in primo luogo, l'ambiente lavorativo estremamente familiare […] La circostanza - che non vuole assurgere ad esimente - ha certamente contribuito ad una gestione meno compliant degli adempimenti privacy; oltre al fatto che il sistema di videosorveglianza era stato originariamente pensato per un uso domestico e soltanto in un

secondo momento si è provveduto all'acquisto della telecamera denominata "ufficio" che, per stessa ammissione del [rappresentante legale della Società], "(…) per praticità di gestione è stata aggiunta all'account" domestico, il cui accesso era, ovviamente, consentito all'intero nucleo familiare del legale rappresentante, nella (corretta) convinzione che il trattamento di dati personali, da parte di una persona fisica nel corso di una attività puramente personale o domestica, non rientra nell'ambito di applicazione del GDPR (art. 2, par. 2 lettera c GDPR). In realtà, tale c.d. "esenzione familiare", nel contesto della videosorveglianza, si sarebbe dovuta interpretare in maniera maggiormente restrittiva, come relativa alle sole attività svolte nel corso della vita privata o familiare delle persone, anche se, giova rammentare che, nel caso di specie, il dato trattato non è stato reso accessibile ad alcuno" (v. nota cit., p. 9);

- "massimo è stato lo spirito di collaborazione con l'Autorità da parte del Titolare del trattamento che, in seguito alla ispezione: a) in ossequio alle previsioni di cui al Provvedimento in materia di videosorveglianza - 08.04.2010 [1712680], ha predisposto un sistema di c.d. "pre-informativa", tramite il quale è possibile garantire gli interessati circa la possibilità di essere informati nel momento in cui stanno per accedere ad una zona videosorvegliata. È stata, pertanto, predisposta una cartellonistica affissa in prossimità della telecamera denominata "ufficio", recante le informazioni più utili ed immediate per gli individui. […] La predetta informativa è stata collocata prima del raggio di azione della telecamera; dunque, nelle sue immediate vicinanze. Essa risulta chiaramente visibile in ogni condizione di illuminazione ambientale ed ingloba un simbolo stilizzato di esplicita ed immediata comprensione per l'interessato. Laddove l'informativa c.d. semplificata da sola non dovesse essere sufficiente, il Titolare del trattamento, sin da ora, si rende disponibile a garantire la consultazione anche del testo completo dell'informativa, con tutte le precisazioni indicate dall'art. 13 GDPR, mediante affissione in apposita bacheca; […] si è attivato per

integrare il sistema di gestione della protezione dei dati al fine di minimizzare e mitigare il rischio di violazioni ed incidenti sui dati personali trattati in Azienda ([…] estratto Registro trattamenti aggiornato, rispettivamente, alla data del 08.11.2021 e del 15.12.2021)" (v. nota cit., p. 9, 10);

- in merito al sistema di rilevazione geografica "la questione […] si presenta altamente problematica dal momento che impone di bilanciare una serie di contrapposti interessi: quelli dell'azienda e quelli dei singoli lavoratori" (v. nota cit., p. 12);

- "la condotta del Titolare - lungi dall'essere stata funzionale al controllo capillare del lavoratore - è dipesa, fondamentalmente, dalla necessità di contabilizzare la durata degli interventi tecnici presso la clientela, onde evitare contestazioni in sede di fatturazione. Ed è questa la ragione per cui […] questo modello sia riconducibile, de plano, alle particolari esigenze organizzative" (v. nota cit., p. 13);

- "il Titolare, pur non avendo puntualmente osservato le garanzie previste in seno allo Statuto, si è adoperato al fine di predisporre apposite cautele volte a proteggere la vita privata dei lavoratori. […] a) il Titolare ha determinato le finalità da perseguire, cui è conseguita una configurazione del sistema applicativo che consentisse il trattamento dei dati in termini di proporzionalità e minimizzazione. La circostanza, poi, che il software GPS utilizzato fosse di "produzione propria" - in quanto ideato e progettato da una risorsa aziendale - ha consentito di non ricorrere a risorse esterne e di calibrare il proprio applicativo al trattamento, per impostazione predefinita, dei soli dati personali necessari alla specifica finalità del trattamento (esatta contabilizzazione delle prestazioni lavorative rese all'esterno); b) le uniche informazioni visibili, a mezzo applicativo, erano quelle riferite ai singoli interventi. La posizione geografica risulta tracciata solo ad applicativo attivato, tanto è vero che, da un controllo a campionatura in sede di ispezione, non è risultato alcuna irregolarità sull'utilizzo del dato posizionale del lavoratore; c) all'applicativo era preclusa la

possibilità di accedere alla messaggistica personale del lavoratore" (v. nota cit., p. 13);

- "certamente, anche in questo caso, il Titolare del trattamento ha peccato di ingenuità - ritenendo di aver correttamente adempiuto al proprio obbligo di trasparenza nei confronti degli interessati, mediante comunicazione orale (e pur sempre nel rispetto delle previsioni di cui all'art. 12 GDPR) - quando, invece, avrebbe dovuto predisporre una modalità di comunicazione intellegibile, trasparente e facilmente accessibile. Circostanza, quest'ultima, a cui è stato posto rimedio" (v. nota cit., p. 13, 14);

- in merito al sistema di rilevazione delle impronte digitali "il Garante - con Provvedimento generale prescrittivo in tema di biometria del 12.11.2014 - ha fornito delle Linee Guida, con riferimento al corretto utilizzo delle c.d. tecniche biometriche […]. Le Linee Guida contemplano anche talune ipotesi di esonero da tale obbligo di verifica preliminare da parte del Garante" (v. nota cit., p. 16);

- "in particolare, in tema di impronte digitali, il Provvedimento del Garante del 12.11.2014 di cui sopra, non richiede al datore di lavoro di ottenere il previo consenso, da parte dei lavoratori, per l'installazione di alcune tecnologie biometriche. Tuttavia, il datore di lavoro/Titolare del trattamento è, in ogni caso, tenuto a comunicare, ai propri lavoratori dipendenti, quali siano i loro diritti, le finalità sottese alla installazione dei suddetti strumenti e quali siano le modalità di trattamento dei dati biometrici raccolti" (v. nota cit., p. 17);

- "le informazioni ai lavoratori in merito alla finalità ed alle modalità di trattamento del dato biometrico sono state rese anche se soltanto in forma orale, in virtù di quella familiarità dei rapporti che contraddistingue il lavoro in Ew Business […]; il Titolare non ha avuto mai accesso alle impronte digitali registrate a sistema; la mancata corrispondenza tra il numero di impronte rilevate (27) ed il numero dei soggetti abilitati (21) è dipesa dal fatto che alcuni lavoratori sono

abilitati a diversi rilevatori; il Titolare del trattamento si è informato sulle modalità di trattamento del dato biometrico operato dalla Società Teycos S.r.l. […], ricevendone comunicazione dalla quale si evince che "(…) nessuna impronta in chiaro viene memorizzata nel terminale, né tanto meno nella centrale di gestione"" (v. nota cit., p. 17);

-"quanto precede non vuole certamente costituire una esimente, per la EW Business, ma denota una necessità cui l'Azienda aveva, in realtà, già posto mano - e che prosegue anche nel mentre ci si accinge alla stesura delle presenti note - circa l'opportunità di coordinare la disciplina statutaria di cui alla Legge n. 300/1970 (c.d. Statuto dei Lavoratori) con la normativa, comunitaria e nazionale, in tema di privacy" (v. nota cit., p. 18);

- "già prima della notifica del Garante - il Titolare del trattamento si era attivato con la Società Teycos S.r.l. per l'adozione di sistemi alternativi a quello di rilevazione delle impronte digitali - ritenuto certamente necessario, ma al contempo foriero di criticità - di cui, peraltro, aveva finanche avviato la sperimentazione. Il riferimento è al "sistema di tag" installato in data 29.10.2021 che, nelle previsioni del Titolare del trattamento - e sempre subordinando le proprie valutazioni ai rilievi che il Garante vorrà svolgere al riguardo - dovrebbe andare a sostituire il rilevamento di impronte digitali associato al sistema di allarme […]. Sistema - quello di rilevazione delle impronte digitali - che, preso atto dei rilievi formulati in sede di ispezione, è stato oggetto di disinstallazione" (v. nota cit., p. 18);

- "sicuramente, l'odierna esponente ha anche difettato nella adeguata informazione da fornire ai propri lavoratori dipendenti, ma con la medesima sicurezza può dirsi che la circostanza non è da ricondursi ad ipotetici intenti persecutori e/o di monitoraggio del lavoratore" (v. nota cit., p. 18);

- "rileva, invece, individuare […] come l'Azienda odierna esponente abbia preso piena consapevolezza della criticità e si sia attivata nella direzione di garantire un processo di interazione continua (in senso bilaterale) tra la disciplina generale sul trattamento dei dati personali (anche particolari ex art. 9 GDPR) e quella specialistica dello Statuto dei Lavoratori" (v. nota cit., p. 18);

- "si confida nella circostanza di aver correttamente adempiuto all'onere di provare di aver agito in assenza di colpevolezza (art. 3 Legge n. 689/1981)" (v. nota cit., p. 20);

- "nelle circostanze concrete del caso che qui occupa, le violazioni contestate non hanno creato un rischio significativo per i diritti degli interessati né, tanto meno, hanno inciso sull'essenza dell'obbligo in questione; […] non ricorre, nel caso di specie, un trattamento improntato al carattere doloso; il numero di interessati coinvolti è davvero esiguo; il grado di cooperazione garantito dal Titolare, al fine di porre rimedio alla violazione ovvero attenuarne i possibili effetti negativi, è stato (ed è) massimo; le misure adottate dal Titolare del trattamento per attenuare gli effetti eventualmente pregiudizievoli in danno degli interessati sono state oltremodo efficaci; non risulta l'irrogazione di precedenti provvedimenti ex art. 58, par. 2 GDPR, nei confronti del medesimo Titolare" (v. nota cit., p. 20, 21).

## 3. L'esito dell'istruttoria.

All'esito dell'esame delle dichiarazioni rese all'Autorità nel corso del procedimento nonché della documentazione acquisita, risulta che la Società, in qualità di titolare, ha effettuato alcune operazioni di trattamento, riferite ai propri dipendenti, che risultano non conformi alla disciplina in materia di protezione dei dati personali, in particolare con riferimento al trattamento dei dati di geolocalizzazione, attraverso un applicativo installato sugli smartphone in uso agli stessi, quindi con riferimento al trattamento dei dati per mezzo di un sistema di videosorveglianza, nonché relativamente al trattamento dei dati biometrici

(impronte digitali) per l'attivazione e la disattivazione di un sistema d'allarme.

In proposito si evidenzia che, salvo che il fatto non costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante".

### 3.1. Trattamento di dati biometrici.

È stato accertato che la Società ha fatto installare, presso la propria sede legale, un sistema di allarme che si attiva e si disattiva attraverso l'uso di impronte digitali.

Il predetto sistema è stato in funzione dal settembre 2019 fino al 29 ottobre 2021, data in cui è stato fatto installare un sistema alternativo ("sistema tag") che non tratta dati biometrici ed è stato "cancellato il database di riferimento per attivazione/disattivazione impianto" (all. 4, 5 scritti difensivi 23.12.2021).

È emerso, in particolare, che il predetto sistema è costituito da una centrale e da tre rilevatori di impronte digitali che consentono di gestire l'allarme nell'ambiente in cui è stato installato.

Sulla base di quanto rilevato in occasione dell'accesso al sistema effettuato durante l'accertamento ispettivo, è risultato che nello stesso sono stati memorizzati i dati relativi alle impronte digitali di 21 soggetti abilitati (tra cui dipendenti della Società, di alcuni sono state rilevate più impronte digitali) e che sono registrati i log riferiti all'attivazione e disattivazione dell'allarme e di accesso al sistema.

È stato anche accertato che per ogni utente in relazione al quale viene conservata l'impronta digitale sono indicati il nome, l'ambiente per cui è abilitato all'accesso e l'indicazione delle dita rilevate.

A differenza di quanto sostenuto dalla Società, risulta accertato che quest'ultima ha trattato dati biometrici dei propri dipendenti, in assenza di un'idonea base giuridica, posto che, come chiarito dall'Autorità, vi è trattamento di tale tipologia di dati sia nella fase di registrazione (c.d. enrollment, consistente nella acquisizione delle caratteristiche biometriche - nella specie impronte digitali - dell'interessato; vi è trattamento di dati biometrici quando viene trattato il dato nella forma di campione biometrico nonché quando viene trattato in forma di modello biometrico; v. punti 6.1 e 6.2 dell'allegato A al provvedimento del Garante del 12 novembre 2014, n. 513, in www.garanteprivacy.it, doc. web n. 3556992), sia nella fase di riconoscimento biometrico, nel caso di specie all'atto dell'attivazione e della disattivazione del sistema d'allarme (v. anche punto 6.3 dell'allegato A al citato provvedimento).

Ciò anche alla luce della definizione di dati biometrici fornita dal Regolamento ("dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici", art. 4, n. 14, del Regolamento) che ha altresì inserito tale tipologia di dati tra i dati appartenenti a categorie particolari di dati (art. 9, par. 1 del Regolamento).

In proposito si osserva che, in base alla disciplina posta in materia di protezione dei dati personali, il trattamento di dati biometrici (di regola vietato ai sensi del richiamato art. 9, par. 1 del Regolamento) è consentito esclusivamente qualora ricorra una delle condizioni indicate dall'art. 9, par. 2 del Regolamento e, con riguardo ai trattamenti effettuati in ambito lavorativo, solo quando il trattamento sia "necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e

protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato" (art. 9, par. 2, lett. b), del Regolamento; v. pure, art. 88, par. 1 e cons. 51-53 del Regolamento).

Affinché, quindi, il trattamento dei dati biometrici, in ambito lavorativo, sia consentito, la fattispecie deve innanzitutto rientrare nelle ipotesi in cui il trattamento sia "necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro [e della sicurezza sociale e protezione sociale]" (v. pure art. 88, par. 1, Regolamento). Tale elemento non ricorre nel caso di specie, considerato che il trattamento dei dati biometrici era finalizzato all'attivazione e alla disattivazione di un sistema di allarme installato presso la sede legale della Società.

Tra l'altro, si precisa che il trattamento dei dati biometrici è consentito solo "nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri […] in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato" (art. 9, par. 2, lett. b), e cons. nn. 51-53 del Regolamento).

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

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. 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).

Alla luce del richiamato quadro normativo il trattamento di dati biometrici realizzato dalla Società risulta quindi essere stato effettuato in assenza di un'idonea base giuridica.

Inoltre, sempre in merito al trattamento dei dati biometrici, è stato accertato che la Società non ha fornito un'idonea informativa agli interessati ai sensi dell'art. 13 del Regolamento.

In proposito la Società ha dichiarato che "in considerazione della relazione che ci è stata fornita […] e, quindi, da quanto riportato nella stessa con la frase "nessuna impronta in chiaro viene memorizzata nel terminale né tantomeno nella centrale di gestione", non si è ritenuto di effettuare alcun trattamento di dati personali; pertanto i nostri dipendenti sono stati informati verbalmente circa la finalità e l'utilizzo del suddetto sistema, con l'indicazione specifica che nessun dato sarebbe rimasto in memoria".

Tra l'altro la stessa Società ha dichiarato di avere "difettato nella adeguata informazione da fornire ai propri lavoratori dipendenti" (v. scritti difensivi nota cit., p. 18).

Come chiarito dall'art. 12 del Regolamento "il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 […] in forma concisa, trasparente, intelligibile e facilmente accessibile […]. Le informazioni sono fornite per iscritto o con altri mezzi, anche se del caso, con mezzi elettronici".

Le informazioni possono essere fornite oralmente solo "se richieste dall'interessato", circostanza che non ricorre nel caso di specie.

La Società, per i motivi suesposti, ha pertanto violato gli artt. 5, par. 1, lett. a), 9, par. 2, lett. b) del Regolamento e dell'art. 13 del Regolamento dalla data di installazione e messa in funzione del sistema di allarme mediante trattamento dei dati biometrici, fino alla sua disinstallazione e sostituzione nel 29 ottobre 2021.

Alla luce dei chiarimenti forniti, non si ritiene invece sussistente la violazione dell'art. 6 del Regolamento, contenuta nella notifica di violazione del 29 novembre 2021, che deve intendersi pertanto archiviata.

### 3.2. Trattamento di dati relativi alla posizione geografica.

È risultato, inoltre, che la Società richiede, al proprio personale tecnico (quantomeno nel numero di 6 tecnici al momento dell'accertamento ispettivo, v. all. 3 ai verbali di operazioni compiute), di utilizzare l'applicativo "eWBM AT", installato sugli smartphone in dotazione ai lavoratori quando svolgono l'attività lavorativa all'esterno della sede aziendale.

Attraverso il predetto applicativo è risultata tracciata, tramite GPS, la posizione del dispositivo mobile sul quale viene scaricato l'applicativo

predetto, in modo continuativo quando il tecnico usa l'applicativo (quindi non quando l'applicativo non è attivo o quando è in background, v. dichiarazione dell'amministratore di sistema secondo cui "il sistema traccia la posizione geografica dell'Iphone, previo accesso all'app, e a condizione che la stessa sia attiva; quindi, in caso di app in back ground piuttosto che con smartphone in standby il sistema non effettua il tracciamento", v. verbale operazioni compiute del 22.6.2021), comunque all'interno del periodo temporale compreso dal lunedì al venerdì, dalle 8 alle 18.

Oltre al dato relativo alla posizione geografica, risultano essere stati raccolti anche il dato relativo all'ora e alla data della rilevazione della posizione stessa, tra l'altro anche dati relativi a periodi molto risalenti nel tempo (2014). È stato inoltre accertato che la Società raccoglie anche gli specifici dati relativi alla posizione geografica, alla data e all'ora della chiusura dell'intervento svolto dal tecnico.

In tal modo risulta tracciata, in modo continuativo, la posizione del lavoratore nello svolgimento della propria attività lavorativa quando l'applicativo risulta in uso.

Tale condotta si pone in contrasto con la disciplina di settore in materia di controlli a distanza (cfr. artt. 5, par. 1, lett. a) del Regolamento in relazione agli artt. 114 del Codice e 4, legge 20.5.1970, n. 300).

Questa disciplina infatti, pure a seguito delle modifiche disposte con l'art. 23 del decreto legislativo 14 settembre 2015, n. 151, non consente l'effettuazione di attività idonee a realizzare il controllo massivo, prolungato e indiscriminato dell'attività del lavoratore (v. Provvedimento generale in materia di localizzazione dei veicoli aziendali cit., spec. par. 3; si vedano anche Article 29 Working Party, Opinion 2/2017 on data processing at work, WP 249, spec. n. 5.7. e Consiglio di Europa, Raccomandazione del 1 aprile 2015, CM/Rec(2015)5, spec. n. 16).

In particolare, i trattamenti di dati personali effettuati nell'ambito del rapporto di lavoro, se necessari per la finalità di gestione del rapporto stesso (v. artt. 6, par. 1, lett. c); 9, par. 2, lett. b) del Regolamento), devono svolgersi nel rispetto dei principi generali indicati dall'art. 5 del Regolamento, ed in particolare del principio di liceità, in base al quale il trattamento è lecito se è conforme alle discipline di settore applicabili (art. 5, par. 1, lett. a) del Regolamento).

Coerentemente con tale impostazione, l'art. 88 del Regolamento ha fatto salve le norme nazionali di maggior tutela ("norme più specifiche") volte ad assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei lavoratori.

Il legislatore nazionale ha approvato, quale disposizione più specifica, l'art. 114 del Codice che tra le condizioni di liceità del trattamento ha stabilito l'osservanza di quanto prescritto dall'art. 4, legge 20 maggio 1970, n. 300. La violazione del richiamato art. 88 del Regolamento è soggetta, ricorrendone i requisiti, all'applicazione di una sanzione amministrativa pecuniaria ai sensi dell'art. 83, par. 5, lett. d) del Regolamento.

In base al richiamato art. 4 della l. n. 300 del 1970, gli strumenti dai quali derivi "anche la possibilità di controllo a distanza" dell'attività dei dipendenti, "possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale" e la relativa installazione deve, in ogni caso, essere eseguita previa stipulazione di un accordo collettivo con la rappresentanza sindacale unitaria o con le rappresentanze sindacali aziendali o, ove non sia stato possibile raggiungere tale accordo o in caso di assenza delle rappresentanze, solo in quanto preceduta dal rilascio di apposita autorizzazione da parte dell'Ispettorato del lavoro.

L'attivazione e la conclusione di tale procedura di garanzia è dunque condizione indefettibile per l'installazione di sistemi di videosorveglianza.

La violazione di tale disposizione è penalmente sanzionata (v. art. 171 del Codice).

Il sistema utilizzato viola, inoltre, il principio di minimizzazione dei dati, enunciato dall'art. 5, par. 1, lett. c) del Regolamento, considerato che, in base allo stesso, il titolare del trattamento deve trattare dati "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati".

La Società, in proposito, ha infatti dichiarato che "non si era a conoscenza di un tracciamento continuo durante l'uso dell'app sugli [smartphone] in dotazione ai tecnici, ma eravamo al corrente della sola rilevazione all'atto della chiusura della chiamata […] e che è utile alla società per far fronte ad eventuali lamentele/contestazioni da parte dei clienti circa la durata dell'intervento tecnico; per queste ragioni non si è ritenuto di dover prendere in considerazione le previsioni di cui allo Statuto dei lavoratori" (v. verbale operazioni compiute 22.6.2021), e che il trattamento dei dati relativi alla posizione geografica deriva "dalla necessità di contabilizzare la durata degli interventi tecnici presso la clientela, onde evitare contestazioni in sede di fatturazione" (v. scritti difensivi del 23.12.2021).

Le stesse dichiarazioni della Società confermano la sproporzione dei dati trattati relativamente alla rilevazione della posizione geografica (unitamente alla data e all'ora della rilevazione) rispetto alla finalità per la quale vengono raccolti gli stessi.

Il dato relativo alla posizione geografica, infatti, non risulta raccolto solo nel momento della "chiusura della chiamata", come la Società ha dichiarato di ritenere e del quale ha bisogno per esigenze organizzative e produttive, ma per tutto il tempo in cui l'applicativo risulta attivo e il tecnico risulta avere acceduto allo stesso (in ogni caso all'interno del periodo temporale compreso dal lunedì al venerdì, dalle 8 alle 18).

Inoltre, con riferimento a questo specifico trattamento, non risulta neanche essere stata fornita un'idonea informativa agli interessati, in

violazione di quanto previsto dall'art. 13 del Regolamento.

In proposito non si può ritenere sufficiente, infatti, la laconica indicazione presente nell'app (v. screenshot acquisiti in sede di ispezione) in base alla quale viene precisato che "questa app traccia la posizione dell'utente ai fini di gestione e controllo aziendale. La tracciatura avviene dal lun al ven, dalle 8.00 alle 18.00" e ancora che l'opzione "posizione esatta" "consente all'app di utilizzare la tua posizione esatta. Quando l'opzione non è attiva, le app potranno determinare soltanto la posizione approssimativa".

La stessa Società ha in proposito dichiarato di avere "peccato di ingenuità - ritenendo di aver correttamente adempiuto al proprio obbligo di trasparenza nei confronti degli interessati, mediante comunicazione orale (e pur sempre nel rispetto delle previsioni di cui all'art. 12 GDPR) - quando, invece, avrebbe dovuto predisporre una modalità di comunicazione intellegibile, trasparente e facilmente accessibile" (v. scritti difensivi 23.12.2021, p. 13, 14).

Non si ritiene, inoltre, sia stato dato adempimento all'obbligo di fornire un'adeguata informativa in merito al trattamento dei dati relativi alla posizione geografica, neanche successivamente all'accertamento ispettivo, considerato che la documentazione fornita con gli scritti difensivi (v. all. 3 agli scritti difensivi del 23.12.2021), datata 9 dicembre 2021, non può considerarsi conforme a quanto prescritto dall'art. 13 del Regolamento; nella stessa documentazione, infatti, risulta solo precisato che "come già comunicatole verbalmente al momento della messa in funzione dell'APP di gestione assistenza tecnica, si conferma che la geolocalizzazione, necessaria alla fatturazione degli interventi tecnici eseguiti, dovrà essere da voi spenta tramite apposito flag al termine della normale giornata lavorativa". Alcuna informazione specifica in merito al trattamento dei dati relativi alla posizione geografica è stata fornita.

Nell'ambito del rapporto di lavoro l'obbligo di informare il dipendente è

altresì espressione del dovere di correttezza ex art. 5, par. 1, lett. a) del Regolamento.

Per le ragioni indicate, la condotta tenuta dalla Società comporta la violazione degli artt. 114 del Codice, 5, par. 1, lett. a), c), 13 e 88 del Regolamento.

### 3.3. Trattamento di dati mediante un sistema di videosorveglianza.

Con riferimento al sistema di videosorveglianza installato presso la sede della Società, è stato accertato che, dall'uso del predetto sistema, può derivare un controllo a distanza dell'attività lavorativa: in particolare, è stato accertato che il legale rappresentante della Società, attraverso il proprio smartphone, può visionare, in diretta, quanto ripreso dalla telecamera che inquadra la postazione adibita a reception, quindi l'attività dei lavoratori che lavorano e transitano nell'area ripresa.

Nonostante ciò, la Società ha dichiarato "che non c'è alcun accordo sindacale in quanto non ci sono rappresentanze in azienda né l'autorizzazione preventiva della Direzione Territoriale del Lavoro circa l'installazione e l'utilizzo della telecamera" (v. verbale di operazioni compiute 21.6.2021).

È stato altresì verificato che il sistema può captare anche i suoni, oltre alle immagini, e consente la registrazione di quanto ripreso. Attraverso l'applicativo è infatti possibile "ammonire verbalmente, attraverso lo speaker della telecamera".

È stato inoltre accertato che l'accesso al sistema di videosorveglianza è consentito a quattro account, dei quali uno risulta intestato alla moglie del rappresentante legale della società, uno al rappresentante legale della Società e due ai figli di quest'ultimo.

Non sono stati riscontrati cartelli contenenti la c.d. informativa breve nei pressi del raggio di azione della telecamera citata, né risulta essere stata fornita ai lavoratori un'informativa completa.

La Società, in proposito, ha dichiarato di avere fornito oralmente un'informativa sul trattamento dei dati mediante il sistema di videosorveglianza, senza essere tuttavia in grado di comprovare questa affermazione.

Ciò risulta in contrasto con quanto prescritto dall'art. 114 del Codice (che richiama l'art. 4 della L. 20.5.1970, n. 300 che disciplina i c.d. controlli a distanza), considerato che, nel caso di installazione di un impianto di videosorveglianza dal quale derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, è necessario il rispetto della specifica procedura descritta normativamente volta ad ottenere, in caso di assenza di rappresentanze sindacali aziendali, il rilascio di una apposita autorizzazione da parte dell'Ispettorato del lavoro.

Tale disciplina lavoristica costituisce una delle norme del diritto nazionale "più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro" individuate dall'art. 88 del Regolamento.

La condotta tenuta dalla Società configura pertanto la violazione del principio di liceità del trattamento (art. 5, par. 1, lett. a) del Regolamento in relazione all'art. 114 del Codice) e dell'art. 88 del Regolamento quanto alla disciplina applicabile in materia.

Il non avere, inoltre, rispettato l'obbligo di fornire un'adeguata informativa agli interessati in merito al trattamento effettuato attraverso l'impianto di videosorveglianza costituisce violazione di quanto disposto dall'art. 13 del Regolamento: in base a tale norma il titolare è tenuto a fornire preventivamente all'interessato tutte le informazioni relative alle caratteristiche essenziali del trattamento.

Nell'ambito del rapporto di lavoro l'obbligo di informare il dipendente è altresì espressione del dovere di correttezza ex art. 5, par. 1, lett. a) del Regolamento.

Con riferimento al nuovo cartello informativo di cui è stata inviata la relativa documentazione fotografica con gli scritti difensivi del 23.12.2021, si osserva quanto segue.

Considerato che sul predetto cartello viene precisato che "la telecamera risulta sempre spenta - non verranno effettuate registrazioni durante l'orario di lavoro", "sarà attivata per visione dei luoghi nel caso di allarme per tentativo di furto" (all. 1 scritti difensivi del 23.12.2021), si osserva come, quanto nello stesso dichiarato, non risulti supportato da evidenze in merito alla effettiva limitazione della funzionalità del sistema di videosorveglianza esclusivamente in orario non lavorativo, né da evidenze relative alle modalità specifiche attraverso le quali l'attivazione della stessa avvenga solo in occasione di un tentativo di furto.

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

Per i suesposti motivi l'Autorità ritiene che le dichiarazioni, la documentazione e le ricostruzioni fornite dal titolare del trattamento nel corso dell'istruttoria non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano pertanto inidonee a consentire l'archiviazione del presente procedimento, non ricorrendo peraltro alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Il trattamento dei dati personali effettuato dalla Società e segnatamente il trattamento dei dati biometrici, di quelli relativi alla posizione geografica, nonché dei dati dei dipendenti attraverso il sistema di videosorveglianza risulta infatti illecito, nei termini su esposti, in relazione agli artt. 114 del Codice, 5, par. 1, lett. a), c), 9, 13 e 88 del Regolamento.

La violazione, accertata nei termini di cui in motivazione, non può essere considerata "minore", tenuto conto della natura, della gravità e della durata della violazione stessa, del grado di responsabilità e della maniera in cui l'autorità di controllo ha preso conoscenza della violazione (cons. 148 del Regolamento).

Pertanto, visti i poteri correttivi attribuiti dall'art. 58, par. 2 del Regolamento, alla luce del caso concreto:

- per quanto riguarda il sistema di videosorveglianza: si dispone il divieto del trattamento effettuato mediante il sistema di videosorveglianza (art. 58, par. 2, lett. f), Regolamento);

- per quanto riguarda il sistema di rilevamento della posizione geografica del lavoratore: si dispone il divieto di monitoraggio continuo della posizione del lavoratore (art. 58, par. 2, lett. f), Regolamento);

- si dispone l'applicazione di una sanzione amministrativa pecuniaria ai sensi dell'art. 83 del Regolamento, commisurata alle circostanze del caso concreto (art. 58, par. 2, lett. i) Regolamento).

Resta fermo che laddove la Società ritenesse di installare un sistema di videosorveglianza, per scopi di tutela del patrimonio e di sicurezza anche dei lavoratori, dovrà conformarsi alle procedure di garanzia previste dall'art. 4 l. n. 300 del 1970, richiamato dall'art. 114 del Codice, prima dell'attivazione del sistema nonché configurare il sistema di videosorveglianza in modo da consentire l'accesso allo stesso, solo a soggetti autorizzati, escludendo la funzione di captazione dell'audio, a meno che non vi siano specifiche ragioni particolari, adeguatamente documentate; ciò avendo cura di posizionare le telecamere in modo da minimizzare l'inquadramento del lavoratore addetto alla reception; qualora si proceda all'attivazione di un sistema di videosorveglianza, la Società dovrà anche adeguare l'informativa.

Resta inoltre fermo che laddove la Società ritenesse di utilizzare un sistema di rilevazione della posizione geografica del lavoratore per finalità organizzative e produttive, dovrà conformarsi alle procedure di garanzia previste dall'art. 4 l. n. 300 del 1970, richiamato dall'art. 114 del Codice, prima dell'attivazione del sistema; qualora si proceda all'attivazione di un sistema di rilevamento della posizione geografica del lavoratore, la Società dovrà conformare al Regolamento i propri trattamenti con riferimento alla corretta predisposizione dei documenti contenenti l'informativa.

## 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).

All'esito del procedimento, risulta accertato che Ew Business Machines S.p.A. ha violato gli artt. artt. 114 del Codice, 5, par. 1, lett. a), c), 9, 13 e 88 del Regolamento. Per la violazione delle predette disposizioni è prevista l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, lett. a), b), d) del Regolamento, mediante adozione di un'ordinanza ingiunzione (art. 18, l. 24.11.1981, n. 689).

Ritenuto di dover applicare il paragrafo 3 dell'art. 83 del Regolamento laddove prevede che "Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento […] viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave", l'importo totale della sanzione è calcolato in modo da non superare il massimo edittale previsto dal medesimo art. 83, par. 5.

Con riferimento agli elementi elencati dall'art. 83, par. 2 del Regolamento ai fini della applicazione della sanzione amministrativa pecuniaria e la relativa quantificazione, tenuto conto che la sanzione deve "in ogni caso

[essere] effettiva, proporzionata e dissuasiva" (art. 83, par. 1 del Regolamento), si rappresenta che, nel caso di specie, sono state considerate le seguenti circostanze:

a) in relazione alla natura, gravità e durata della violazione, è stata considerata rilevante la natura della violazione che ha riguardato i principi generali del trattamento; le violazioni hanno riguardato anche la disciplina di settore in materia di controlli a distanza nonché il trattamento di dati appartenenti a categorie particolari di dati;

b) con riferimento al carattere doloso o colposo della violazione e al grado di responsabilità del titolare, è stata presa in considerazione la condotta della Società e il grado di responsabilità della stessa che non si è conformata alla disciplina in materia di protezione dei dati, relativamente a una pluralità di disposizioni riguardanti anche i principi generali del trattamento nonché la disciplina di settore in materia di controlli a distanza;

c) a favore della Società si è tenuto conto della cooperazione con l'Autorità di controllo e della assenza di precedenti violazioni pertinenti.

Si ritiene inoltre che assumano rilevanza nel caso di specie, tenuto conto dei richiamati principi di effettività, proporzionalità e dissuasività ai quali l'Autorità deve attenersi nella determinazione dell'ammontare della sanzione (art. 83, par. 1, del Regolamento), in primo luogo le condizioni economiche del contravventore, determinate in base ai ricavi conseguiti dalla Società con riferimento al bilancio abbreviato d'esercizio per l'anno 2021. Da ultimo si tiene conto dell'entità delle sanzioni irrogate in casi analoghi.

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene, nel caso di specie, di applicare nei confronti di Ew Business Machines S.p.A. la sanzione amministrativa del pagamento di una somma pari ad euro 20.000 (ventimila).

In tale quadro si ritiene, altresì, in considerazione della tipologia delle violazioni accertate che hanno riguardato i principi generali del trattamento, la disciplina di settore in materia di controlli a distanza nonché il trattamento di dati appartenenti a categorie particolari di dati, che ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente provvedimento sul sito Internet del Garante.

Si ritiene, altresì, che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

## TUTTO CIO' PREMESSO IL GARANTE

rileva l'illiceità del trattamento effettuato da Ew Business Machines S.p.A., in persona del legale rappresentante, con sede legale in Viale Andrea Doria, n. 17 (MI), C.F. 06172060961, ai sensi dell'art. 143 del Codice, per la violazione degli artt. 114 del Codice, 5, par. 1, lett. a), c), 9, 13 e 88 del Regolamento;

## DETERMINA

di archiviare ai sensi dell'art. 11 comma 1 lett. b) del regolamento interno n. 1 del 2019 la contestazione adottata nei confronti di Ew Business Machines S.p.A., in persona del legale rappresentante, con atto del 29 novembre 2021, limitatamente alla violazione dell'art. 6 del Regolamento;

## DISPONE

ai sensi dell'art. 58, par. 2, lett. f) del Regolamento, a Ew Business Machines S.p.A. il divieto del trattamento effettuato mediante il sistema di videosorveglianza nonché il divieto di monitoraggio continuo della posizione del lavoratore nei termini indicati in motivazione;

## INGIUNGE

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

## ORDINA

ai sensi dell'art. 58, par. 2, lett. i) del Regolamento a Ew Business Machines S.p.A. di pagare la predetta somma di euro 20.000 (ventimila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento;

## DISPONE

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

Richiede a Ew Business Machines S.p.A. di comunicare quali iniziative siano state intraprese al fine di dare attuazione a quanto disposto con il presente provvedimento e di fornire comunque riscontro adeguatamente documentato ai sensi dell'art. 157 del Codice, entro il termine di 90 giorni dalla data di notifica del presente provvedimento; l'eventuale mancato riscontro può comportare l'applicazione della sanzione amministrativa prevista dall'art. 83, par. 5, lett. e) del Regolamento.

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

*Roma, 1° giugno 2023*

IL PRESIDENTE
Stanzione

IL RELATORE
Cerrina Feroni

IL SEGRETARIO GENERALE
Mattei