Provvedimento del 10 aprile 2025 [10139433]

[doc. web n. 10139433]

Provvedimento del 10 aprile 2025

Registro dei provvedimenti
n. 201 del 10 aprile 2025

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, "Regolamento generale sulla protezione dei dati" (di seguito, "Regolamento");

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

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

Vista la documentazione in atti;

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

Relatore il prof. Pasquale Stanzione;

PREMESSO

1. Introduzione.

Con reclamo presentato ai sensi dell'art. 77 del Regolamento, il Sig. XX, dipendente dell'Unione Montana Appennino Parma Est (di seguito, l'"Unione"), in servizio presso il XX, ha lamentato - sia in proprio sia in quanto esercente la responsabilità genitoriale su un proprio figlio minore - una presunta violazione della disciplina in materia di protezione dei dati personali, riguardante il

trattamento dei dati personali suoi e di suo figlio mediante una telecamera di videosorveglianza.

In particolare, il reclamante ha rappresentato che "l'entrata pedonale del […] Comando [di Polizia locale] è sottoposta a videosorveglianza tramite la presenza di una telecamera esterna attiva 24 h/24 h e 7 gg/7 gg le cui immagini vengono registrate e conservate da parte del Titolare del Trattamento". In tale contesto, l'Unione non avrebbe né apposto un cartello informativo, contenente l'informativa di primo livello sul trattamento dei dati personali, in prossimità della telecamera di videosorveglianza, né fornito agli interessati un'informativa completa di secondo livello; non avrebbe redatto una valutazione d'impatto sulla protezione dei dati (di seguito, "VIPD"), ai sensi dell'art. 35 del Regolamento, prima di iniziare il trattamento; avrebbe impiegato detta telecamera, idonea a riprendere anche gli appartenenti al Corpo di Polizia Locale nel contesto lavorativo, in violazione dell'art. 4 della l. 20 maggio 1970, n. 300; avrebbe conservato i dati personali contenuti nelle immagini di videosorveglianza "più a lungo di quanto necessario per le finalità per le quali sono trattati", atteso che "con riferimento all'accesso [nei locali del Comando di Polizia locale,] effettuato dal reclamante […] in data XX unitamente a suo figlio minore, […] [l'Unione] ha conservato le immagini per un tempo superiore alle 24 ore (le immagini sono state visionate il giorno XX) senza che ricorressero esigenze particolari tali da giustificare un prolungamento della conservazione)".

2. L'attività istruttoria.

In riscontro a una richiesta d'informazioni dell'Autorità (v. nota prot. n. XX del XX), l'Unione, con nota del XX (prot. n. XX), ha dichiarato, in particolare, che:

> "la telecamera di videosorveglianza in questione è stata installata e messa in funzione nel mese di febbraio dell'anno 2016";
>
> "la finalità di trattamento perseguita […] nell'ambito dell'azione di sicurezza urbana integrata è la tutela degli immobili di proprietà o in gestione dell'Amministrazione […]. [La] base giuridica [del trattamento è da ricondursi all'] […] art. n. 6 comma 1 lettera e) del [Regolamento] […]";
>
> "la telecamera […] riprende esclusivamente l'area di accesso agli uffici e in campo lungo l'area di sosta dei veicoli di proprietà e alcuna attività svolta dai lavoratori; essendo la finalità quella nell'ambito dell'azione di sicurezza urbana integrata di tutela degli immobili di proprietà o in gestione dell'Amministrazione, non si rientra nell'ambito di applicazione dell'art. 4 della L. n. 300/70. Per tale ragione non è stato stipulato un accordo con le organizzazioni sindacali né richiesta l'autorizzazione all'Ispettorato Territoriale del Lavoro";
>
> "sulla base delle disposizioni normative vigenti, […] il termine massimo di conservazione dei dati è di 7 giorni […]";
>
> è stato apposto un "cartello con l'informativa di 1° livello […] in prossimità della telecamera in questione nel mese di settembre dell'XX. L'informativa estesa sul trattamento dei dati è disponibile agli interessati sul sito istituzionale dell'Unione […] nella sezione Unione – Privacy";
>
> "è stata redatta una […] valutazione d'impatto sulla protezione dei dati […];
>
> "circa la circostanza [che] il filmato che ritrae il reclamante ed un proprio figlio minore, acquisito in data XX, sarebbe stato conservato quantomeno fino al XX […] si pone in evidenza come in data XX siano stati acquisiti in atti, nell'ambito di un procedimento disciplinare verso l'interessato, semplicemente i report di stampa degli accessi agli uffici del comando […] risultanti dalla disattivazione e riattivazione del sistema di allarme […]".

In riscontro a una seconda richiesta d'informazioni dell'Autorità (v. nota prot. n. XX del XX, l'Unione, con nota del XX (prot. n. XX), ha dichiarato, in particolare, che:

> dai "report di stampa degli accessi agli uffici del Comando risultanti dalla disattivazione e riattivazione del sistema di allarme […] si evince come il sistema di allarme in data XX sia stato spento all'ingresso mattutino del personale alle ore 06:56 per essere poi attivato al termine della giornata lavorativa alle ore 19:09. Nella medesima data è stato poi disattivato alle ore 20:02 per essere riattivato alle ore 20:53";
>
> la VIPD è stata formalizzata con "determinazione dirigenziale n. XX del XX", oggetto di pubblicazione nell'Albo Pretorio dell'Ente;
>
> l'Unione ha stipulato un "patto per l'attuazione della sicurezza urbana […] con la Prefettura di Parma in data XX comprendente Via Cascinapiano, ove è situata la sede del Comando della Polizia Locale".

Con nota del XX (prot. n. XX), l'Ufficio, sulla base degli elementi acquisiti, dalle verifiche compiute e dei fatti emersi a seguito dell'attività istruttoria, ha notificato all'Unione, ai sensi dell'art. 166, comma 5, del Codice, l'avvio del procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento:

> per aver posto in essere un trattamento di dati personali dei lavoratori, mediante la telecamera di videosorveglianza in questione, in contrasto con la normativa in materia di protezione dei dati personali e con la disciplina di settore in materia di controlli a distanza, nonché per aver trattato i dati personali del reclamante e del proprio figlio minore, raccolti mediante detta telecamera, nell'ambito di un procedimento disciplinare, in assenza dei necessari presupposti di liceità, in violazione degli artt. 5, par. 1, lett. a) e b), 6, e 88 del Regolamento, nonché 114 del Codice, in riferimento all'art. 4, della l. 20 maggio 1970, n. 300;
>
> per non aver assicurato la necessaria trasparenza del trattamento nei confronti degli interessati, con conseguente violazione degli artt. 5, par. 1, lett. a), 12 e 13 del Regolamento;
>
> per non aver redatto una VIPD in relazione al trattamento dei dati personali dei lavoratori posto in essere mediante la medesima telecamera, in violazione dell'art. 35 del Regolamento.

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

Con nota del XX (prot. n. XX), l'Unione ha presentato una memoria difensiva, dichiarando, in particolare, che:

> l'Unione "si è fatta immediatamente parte attiva per concludere il percorso di definizione con le OOSS di un "Accordo relativo alla videosorveglianza ai sensi dell'art. 4 della legge n. 300/1970" […], che è stato sottoscritto in data XX con successiva presa d'atto da parte della Giunta dell'Ente con deliberazione n. XX in data XX";
>
> l'Unione "si è fatta immediatamente parte attiva predisponendo un'informativa di secondo livello aggiornata […], approvata con delibera di Giunta di questa Unione n. XX in data XX […] e già pubblicata nel sito istituzionale dell'Ente. È stata inoltre predisposta, pubblicata sul sito istituzionale ed inviata a mezzo mail l'informativa per i dipendenti […] approvata con delibera di Giunta di questa Unione n. XX del XX";

“per quanto attiene il procedimento disciplinare […] [, si evidenzia che] il giorno XX il Comandante della Polizia Locale [ha ricevuto da terzi, per le vie brevi, una segnalazione in merito alla circostanza che] […] l’agente si sarebbe recato presso il comando con il figlio la sera stessa”;

“[…] il giorno XX il Comandante provvedeva tramite mail […] a chiedere conferma [al reclamante] dell’accesso presso il comando”;

“il giorno XX […] il reclamante […] confermava di aver avuto accesso al comando”;

“per accertare la durata della permanenza dell’agente presso il comando il Comandante acquisiva tramite il sistema di allarme il report di stampa degli accessi […], accertando un accesso dalle ore 20,02 alle ore 20,53 del XX”;

“[…] in base a tali elementi, il giorno XX il Comandante provvedeva a trasmettere la segnalazione di violazioni che comportano responsabilità disciplinare all’Ufficio Procedimenti Disciplinari […]. Si evidenzia che la presenza del minore viene solo ipotizzata (“l’accesso sia da ritenersi effettuato con il proprio figlio”) sulla base della segnalazione [effettuata da terzi] e non a seguito di trattamento delle immagini della telecamera”;

l’Unione “si è fatta immediatamente parte attiva e ha provveduto a predisporre la [VIPD] per finalità di tutela del patrimonio aziendale, sicurezza del lavoro ed esigenze organizzative […], con delibera di Giunta di questa Unione n. XX in data XX”;

“la buona fede dell’Ente, è basata sulla convinzione che la videocamera […] rientrasse nell’ambito della sicurezza urbana integrata in quanto esterna rispetto al luogo di lavoro”;

“ad evidenza della volontà dell’Ente nel richiamo all’utilizzo della telecamera all’ambito sicurezza urbana, è rilevabile [dalla documentazione prodotta in atti] che il Patto per l’attuazione della sicurezza urbana stipulato in data XX tra il Comune di Langhirano e la Prefettura di Parma, prodotto in atti, include anche la telecamera oggetto di reclamo, installata presso il Comando della Polizia locale”.

L’Unione non si è, invece, avvalsa del diritto di essere audita presso l’Autorità ai sensi dell’art. 166, comma 6, del Codice.

3. Esito dell’attività istruttoria.

3.1 La liceità del trattamento.

La disciplina in materia di trattamento dei dati personali prevede che i soggetti pubblici possono, di regola, trattare dati personali se il trattamento è necessario “per adempiere un obbligo legale al quale è soggetto il titolare del trattamento” oppure “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, par. 1, lett. c) ed e) del Regolamento e art. 2-ter del Codice).

Con specifico riferimento all’utilizzo di sistemi di videosorveglianza da parte di soggetti pubblici, già nel “Provvedimento in materia di videosorveglianza” (provv. dell’8 aprile 2010, doc. web n. 1712680) il Garante aveva chiarito che tali soggetti, “in qualità di titolari del trattamento […], possono trattare dati personali nel rispetto del principio di finalità, perseguendo scopi determinati, espliciti e legittimi […] per lo svolgimento delle proprie funzioni istituzionali” (par. 5) (cfr., le “Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video” adottate dal Comitato europeo per la protezione dei dati il 29 gennaio 2020, sez. 3.2).

Ciò stante, quando, come nel caso di specie, le telecamere di videosorveglianza sono idonee a

riprendere anche il personale che transita o sosta nei luoghi di lavoro, il trattamento dei dati personali dei lavoratori, da parte del datore di lavoro, può essere effettuato se è necessario, in generale, per la gestione del rapporto di lavoro, nel rispetto del quadro giuridico applicabile, definito dalla normativa nazionale ed eurounitaria, da regolamenti o da contratti collettivi (artt. 6, par. 1, lett. c), e 88 del Regolamento).

In tale quadro, il datore di lavoro deve rispettare le norme nazionali che "includono misure appropriate e specifiche a salvaguardia della dignità umana […] degli interessati in particolare per quanto riguarda la trasparenza del trattamento […] e i sistemi di monitoraggio sul posto di lavoro" (artt. 6, par. 2, e 88, par. 2, del Regolamento).

Per effetto del rinvio contenuto nel Codice alle preesistenti disposizioni nazionali di settore che tutelano la dignità delle persone sul luogo di lavoro, con particolare riferimento ai possibili controlli da parte del datore di lavoro (art. 114 "Garanzie in materia di controllo a distanza"), l'osservanza dell'art. 4 della l. 20 maggio 1970, n. 300 (Statuto dei Lavoratori) costituisce una condizione di liceità del trattamento (cfr. par. 4.1 del citato "Provvedimento in materia di videosorveglianza" dell'8 aprile 2010; v., da ultimo, la FAQ n. 9 del Garante in materia di videosorveglianza, del dicembre 2020, doc. web 9496574 e le numerose decisioni del Garante riferite a casi concreti).

L'art. 4, comma 1, dello Statuto dei Lavoratori stabilisce, infatti, che "gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali […]. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, […] della sede centrale dell'Ispettorato nazionale del lavoro".

Tali garanzie dello Statuto dei Lavoratori trovano, peraltro, applicazione in qualunque contesto lavorativo pubblico e privato, fatto salvo quanto disposto altrimenti dalle specifiche disposizioni di settore (combinato disposto art. 37 della l. 300/1970 e artt. 3, 42 e 51, comma 2, del d.lgs. 165/2001; v. anche C.d.S., sent. n. 708 del 12 luglio 1990 e C.d.S, sez. V, sent. n. 95 del 23 gennaio 1995, in base alle quali le norme della l. n. 300/1970 si applicano ai dipendenti pubblici nel caso in cui manchi del tutto la disciplina relativa al caso di specie nell'ambito dell'ordinamento interno dell'ente).
Ciò premesso, sulla base degli elementi acquisiti e dei fatti emersi a seguito dell'attività istruttoria, risulta accertato che, a partire dal febbraio 2016, l'Unione ha installato una telecamera di videosorveglianza presso la sede della Polizia locale sita in Via Cascinapiano, 1 - 43013 Langhirano (PR), che "riprende esclusivamente l'area di accesso agli uffici e in campo lungo l'area di sosta dei veicoli di proprietà", per finalità "di sicurezza urbana integrata di tutela degli immobili di proprietà o in gestione dell'Amministrazione".

Al riguardo, deve, anzitutto, evidenziarsi che risulta inconferente il richiamo effettuato dall'Unione all'ambito della "sicurezza urbana integrata" in relazione alla telecamera di videosorveglianza in questione. La disciplina di settore consente, infatti, ai Comuni di installare sistemi di videosorveglia per la "prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria", a condizione che sia stipulato un patto per l'attuazione della sicurezza urbana tra Sindaco e Prefettura territorialmente competente (v. artt. 6, co. 7 e 8, del d.l. 23 febbraio 2009, nonché 4 e 5, co. 2, lett. a), del d.l. 20 febbraio 2017, n. 14; cfr. provv.ti 19 dicembre 2024, n. 805, doc. web n. 10107263; 11 gennaio 2024, n. 5, doc. web n. 9977020 e 20 ottobre 2022, n. 341, doc. web n. 9831369).

Tale telecamera di videosorveglianza, riprendendo esclusivamente un ingresso esterno alla sede di Polizia locale e parte del parcheggio delle auto di servizio, non può ritenersi strumentale alla tutela della sicurezza urbana, non potendo ontologicamente assolvere al compito di prevenire e

contrastare gli specifici fenomeni di criminalità diffusa e predatoria, cui fa riferimento la richiamata disciplina di settore, che tipicamente si verificano nella pubblica via (cfr., da ultimo, provv. 11 aprile 2024, n. 234, doc. web n. 10013356). Né rileva, a tal riguardo, che, come dichiarato dall'Unione in sede di memoria difensiva, il patto per l'attuazione della sicurezza urbana stipulato tra il Comune di Langhirano e la Prefettura di Parma in data XX (dunque molti anni dopo la data d'installazione di detta telecamera) menzioni la telecamera in questione, atteso che la stessa non risulta comunque idonea a riprendere la pubblica via ed assolvere alla finalità di tutela di sicurezza urbana (v. la nota dell'Unione del XX, in cui si afferma che "la telecamera [...] riprende esclusivamente l'area di accesso agli uffici e in campo lungo l'area di sosta dei veicoli di proprietà", e l'all. 2 alla stessa, che contiene una schermata esemplificativa dell'angolo di visuale della telecamera).

Stando a quanto dichiarato, l'effettiva finalità perseguita, ovvero la "tutela degli immobili di proprietà o in gestione dell'Amministrazione", impropriamente ricondotta all'ambito della sicurezza urbana, si colloca invece nell'alveo dell'art. 4 della l. 300/1970, ai sensi del quale, come evidenziato, "gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per [...] la tutela del patrimonio aziendale", nel rispetto delle procedure e delle garanzie ivi previste. Tale disposizione trova applicazione in tutti i luoghi e contesti in cui operano o transitano anche lavoratori, circostanza che ricorre nel caso di specie (cfr., da ultimo, provv. n. 331 del 16 settembre 2021, doc. web n. 9719768). In proposito, il Garante ha, infatti, costantemente ritenuto che anche le aree nelle quali transitano o sostano - talora continuativamente - i dipendenti (ad es. accessi alla struttura e ai garage, zone di carico/scarico merci, ingressi carrai e pedonali), qualora sottoposte a videosorveglianza, sono soggette alla piena applicazione della disciplina in materia di protezione dei dati personali e a quella in materia di controlli a distanza (v., tra gli altri, 30 luglio 2015, n. 455, doc. web n. 4261028; 4 luglio 2013, n. 334, doc. web n. 2577203; 18 aprile 2013, n. 199 e 200, doc. web n. 2483269; 9 febbraio 2012, n. 56, doc. web n. 188699; 17 novembre 2011, n. 434, doc. web n. 1859558; 26 febbraio 2009, doc. web n. 1601522).

Come è emerso nel corso dell'istruttoria, l'Unione ha installato e messo in funzione la telecamera di videosorveglianza oggetto di reclamo, fin dal 2016, senza aver previamente esperito le procedure di garanzia di cui all'art. 4, comma 1, della l. 300/1970, non avendo la stessa né stipulato un accordo con le rappresentanze sindacali né ottenuto un'autorizzazione dal competente Ispettorato territoriale del lavoro. Soltanto a seguito dell'avvio del procedimento relativo al reclamo, l'Unione si è, infatti, attivata per la stipula un accordo con le organizzazioni sindacali, poi effettivamente formalizzato in data XX.

A tal riguardo, si evidenzia che le esigenze di tutela del patrimonio aziendale, pure invocate dall'Unione, non possono di per sé sole, in base al quadro normativo sopra delineato, legittimare il trattamento dei dati personali mediante strumenti dai quali può derivare anche la possibilità di controllo a distanza dei lavoratori, come la telecamera di videosorveglianza in questione, in assenza delle garanzie previste dall'art. 4, comma 1, l. n. 300/1970, che definisce, per le ragioni sin qui esposte, limiti, condizioni e presupposti del relativo trattamento.

Sul punto, anche la giurisprudenza della Corte europea dei diritti dell'uomo, nel caso Antovic e Mirkovic v. Montenegro (Application n. 70838/13 del 28.11.2017), ha stabilito che il rispetto della "vita privata" deve essere esteso anche ai luoghi di lavoro pubblici (nel caso di specie, le aule universitarie), evidenziando che la videosorveglianza sul posto di lavoro pubblico può essere giustificata solo nel rispetto delle garanzie previste dalla legge nazionale applicabile, in mancanza delle quali costituisce un'interferenza illecita nella vita privata del dipendente, ai sensi dell'art. 8, par. 2, della CEDU.

Pertanto, il rispetto del citato art. 4, comma 1, anche per effetto del rinvio ad esso contenuto nell'art. 114 del Codice, costituisce condizione di liceità del trattamento dei dati personali (cfr., da

ultimo, con riguardo al ricorso alla videosorveglianza sui luoghi di lavoro, provv.ti 11 aprile 2024, n. 234, doc. web n. 10013356; 16 novembre 2023, n. 578, doc. web n. 9963486; 16 settembre 2021, n. 331, doc. web n. 9719768; 11 marzo 2021, n. 90, doc. web n. 9582791; 5 marzo 2020, n. 53, doc. web n. 9433080; 19 settembre 2019, n. 167, doc. web n. 9147290; v., a livello europeo, le indicazioni contenute nelle citate "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", spec. par. 11, nonché le precedenti indicazioni del Gruppo di Lavoro Articolo 29 nel "Parere 2/2017 sul trattamento dei dati sul posto di lavoro", WP 249; in giurisprudenza, v. Cass. pen., sez. 3, 17 dicembre 2019, n. 50919; Cass. civ., sez. 1, 19 settembre 2016, n. 18302).

In ragione delle considerazioni che precedono, il trattamento dei dati personali posto in essere mediante la predetta telecamera risulta essere stato effettuato in contrasto con la normativa in materia di protezione dei dati personali e con la disciplina di settore in materia di controlli a distanza, ossia in assenza delle procedure di garanzia richieste dalla legge nazionale applicabile, che ne costituisce la base giuridica (sotto tale profilo, ancorché con riferimento all'impiego di diversi sistemi nel contesto lavorativo, v. provv. 1° dicembre 2022, n. 409, doc web n. 9833530, spec. parr. 3.4 e 3.5).

L'impiego di detta telecamera ha, pertanto, comportato il trattamento di dati personali relativi ai lavoratori e ad altri interessati (ad esempio, visitatori, utenti, fornitori, cittadini e altre categorie di interessati), in maniera non conforme al "principio di liceità, correttezza e trasparenza" e in assenza di una base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6 e 88, par. 1, del Regolamento, nonché 114 del Codice (in relazione all'art. 4, comma 1, della l. n. 300/1970).

Devono, invece, considerarsi superate, a seguito della documentazione pervenuta in data XX, le contestazioni mosse all'Unione in merito all'illecito trattamento dei dati ottenuti dalla predetta telecamera per fini disciplinari (cfr. l'art. 4, par. 3, della l. 300/1970), tenuto conto che l'Ente ha dichiarato, con assunzione di responsabilità anche ai sensi dell'art. 168 del Codice, che le immagini di videosorveglianza non sono state utilizzate per comprovare i presunti illeciti disciplinari e che la presenza nella sede del Comando del figlio minore del reclamante è stata soltanto ipotizzata, sulla base di una segnalazione presentata da terzi (v. anche la nota dell'Ufficio procedimenti disciplinari della Provincia di Parma dell'XX, prot. n. XX, in atti, ove si legge che l'"ingresso dell'incolpato [è stato] accertato non a mezzo di telecamere – ma attraverso il sistema di allarme").

3.2. La trasparenza nei confronti degli interessati.

Allorquando siano impiegati dispositivi video, il titolare del trattamento, oltre a rendere l'informativa di primo livello mediante apposizione di segnaletica di avvertimento in prossimità della zona sottoposta a videosorveglianza, deve fornire agli interessati anche delle "informazioni di secondo livello", che devono "contenere tutti gli elementi obbligatori a norma dell'articolo 13 del [Regolamento]" ed "essere facilmente accessibili per l'interessato, ad esempio attraverso un pagina informativa completa messa a disposizione in uno snodo centrale […] o affissa in un luogo di facile accesso" ("Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", cit., in particolare par. 7; ma si veda già il "Provvedimento in materia di videosorveglianza" del Garante dell'8 aprile 2010, cit., in particolare par. 3.1; da ultimo, v. la FAQ n. 4 del Garante in materia di videosorveglianza, cit., cfr., altresì, provv.ti 19 dicembre 2024, n. 805, doc. web n. 10107263 ed i precedenti ivi citati).

Le informazioni di primo livello (cartello di avvertimento) "dovrebbero comunicare i dati più importanti, ad esempio le finalità del trattamento, l'identità del titolare del trattamento e l'esistenza dei diritti dell'interessato, unitamente alle informazioni sugli impatti più consistenti del trattamento" ("Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", cit., par. 114). Inoltre, la segnaletica deve contenere anche quelle informazioni che potrebbero risultare inaspettate per l'interessato. Potrebbe trattarsi, ad esempio, della trasmissione di dati a terzi, in

particolare se ubicati al di fuori dell'UE, e del periodo di conservazione dei dati. Se tali informazioni non sono indicate, l'interessato dovrebbe poter confidare nel fatto che vi sia solo una sorveglianza in tempo reale, senza alcuna registrazione di dati o trasmissione a soggetti terzi (ibidem, cit., par. 115). La segnaletica di avvertimento di primo livello deve contenere un chiaro riferimento al secondo livello di informazioni, ad esempio indicando un sito web sul quale è possibile consultare il testo dell'informativa estesa.

Nel caso di specie, l'Unione ha dichiarato che è stato apposto un "cartello con l'informativa di 1° livello […] in prossimità della telecamera […] nel mese di settembre dell'anno XX" (v. all. 3 alla nota dell'Unione del XX).

Risulta, pertanto, accertato che, nell'intervallo temporale intercorrente tra il mese di febbraio 2016, in cui detta telecamera è stata installata e messa in funzione, e il mese di settembre XX, in cui tale cartello è stato collocato, l'Unione non ha fornito agli interessati alcuna informativa di primo livello sul trattamento dei dati.

Quanto al periodo successivo al mese di settembre XX, deve osservarsi che il cartello informativo affisso risulta essere, tuttavia, inidoneo, in quanto, con riferimento alla finalità perseguita dall'Unione, menzionata le finalità di "sicurezza pubblica – sicurezza urbana – polizia giudiziaria – polizia amministrativa", che come detto non si ritiene possano essere perseguite nel contesto di specie, e non, invece, ovvero la finalità di tutela del patrimonio, come, peraltro, confermato dalla circostanza che codesta Unione, successivamente all'avvio dell'istruttoria, ha stipulato un accordo con le organizzazioni sindacali, ai sensi dell'art. 4 della l. 300/1970.

Inoltre, anche in riferimento all'informativa completa di secondo livello, il cartello in questione rimanda al sito web istituzionale dell'Unione. Il testo di tale informativa prodotto in atti (v. all. 4 alla nota dell'Unione del XX), che reca l'indicazione "ultima modifica XX", fa generico riferimento ai trattamenti di dati personali posti in essere dall'Unione per proprie "finalità istituzionali" e non riguarda, pertanto, i trattamenti posti in essere mediante detta telecamera di videosorveglianza per le finalità di sicurezza sul lavoro e tutela del patrimonio di cui all'art. 4 della l. 300/1970, cui si fa riferimento nell'accordo sindacale concluso in data XX.

L'Unione ha, pertanto, omesso di fornire agli interessati (ad esempio, visitatori, utenti, fornitori, cittadini e altre categorie di interessati) un'idonea informativa estesa, di secondo livello, sul trattamento dei dati personali.

Anche per quanto attiene specificamente al trattamento dei dati personali dei lavoratori mediante il dispositivo video impiegato, l'Unione ha non comprovato di aver fornito agli stessi una specifica informativa sul trattamento dei dati personali connesso al perseguimento della finalità di tutela del patrimonio di cui all'art. 4 della l. 300/1970.

Deve, pertanto, concludersi che l'Unione ha agito in maniera non conforme al "principio di liceità, correttezza e trasparenza" e in violazione degli artt. 5, par. 1, lett. a), 12 e 13 del Regolamento.

3.3 La valutazione d'impatto sulla protezione dei dati.

In attuazione del principio di "responsabilizzazione" (cfr. art. 5, par. 2, e 24 del Regolamento), spetta al titolare valutare se i trattamenti che si intendono realizzare possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche - in ragione delle tecnologie impiegate e considerata la natura, l'oggetto, il contesto e le finalità perseguite - che renda necessaria una preventiva valutazione di impatto sulla protezione dei dati personali ai sensi dell'art. 35 del Regolamento (cfr. cons. 90 del Regolamento).

Nel caso di specie, il trattamento dei dati personali dei lavoratori in servizio presso la Polizia locale dell'Unione, è stato effettuato, mediante la telecamera di videosorveglianza oggetto di reclamo,

anche in assenza di una VIPD.

La copia della VIPD depositata in atti dall'Unione (v. all. 5 alla nota del XX) fa, infatti, riferimento al "trattamento di dati personali di dati personali eseguito con i SDV [, ovvero con i sistemi di videosorveglianza,] per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri", anche ai sensi del "decreto legge 14/2017 [che] ha riconosciuto l'importanza dei sistemi di videosorveglianza come strumento atto a prevenire e contrastare fenomeni di criminalità diffusa e predatoria".

Gli interessati da tali trattamenti sono identificati in "tutte le persone fisiche che transitano nelle aree osservate dai SDV [… che] riguardano aree di pubblico passaggio". I dispositivi di videosorveglianza considerati ai fini di tale VIPD sono i seguenti: "A. rete di telecamere fisse dedicate alla sorveglianza del territorio dell'Unione; B. rete di telecamere fisse dedicate al riconoscimento delle targhe dei veicoli […]; C. telecamere mobili per vigilanza sui rifiuti e finalità di polizia giudiziaria, tra cui le fototrappole; D. telecamere mobili applicabile alle divise degli agenti di Polizia Locale ("bodycam") o sui veicoli di servizio ("dashcam") […]".

Emerge, pertanto, che la VIPD non ha preso in specifica considerazione il trattamento dei dati personali dei lavoratori posto in essere mediante sistemi di videosorveglianza per la tutela del patrimonio aziendale ai sensi dell'art. 4, comma 1, della l. 300/170.

Tenuto conto delle indicazioni fornite anche a livello europeo sul punto, si rileva, invece, che tale trattamento comporta rischi specifici per i diritti e le libertà degli interessati nel contesto lavorativo (art. 35 del Regolamento; cfr. provv. 16 novembre 2023, n. 578, doc. web n. 9963486).

Tanto in considerazione della particolare "vulnerabilità" degli interessati nel contesto lavorativo (cfr. cons. 75 e art. 88 del Regolamento e le "Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679", WP 248 del 4 aprile 2017, che, tra le categorie di interessati vulnerabili, menzionano espressamente "i dipendenti") e del fatto che in tale ambito l'impiego di sistemi che comportano il "monitoraggio sistematico", inteso come "trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti" (cfr. criterio n. 3 indicato nelle Linee guida, cit., ma vedi anche criteri 4 e 7), può presentare rischi in termini di possibile monitoraggio dell'attività dei dipendenti (cfr. artt. 35 e 88, par. 2, del Regolamento; v. anche provv. 11 ottobre 2018, n. 467, doc. web n. 9058979, all. n. 1, che espressamente menziona i "trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici […] dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti"; v., tra gli altri, provv. 1° dicembre 2022, n. 409, doc. web n. 9833530).

La mancata redazione di una valutazione d'impatto in relazione a sistemi di videosorveglianza impiegati nel contesto lavorativo è stata oggetto di recenti provvedimenti anche correttivi e sanzionatori del Garante (v. in particolare, provv.ti 16 novembre 2023, nn. 577 e 578, doc. web n. 9963486; v. anche Newsletter 15 dicembre 2023, doc. web n. 9963533).

Nel caso di specie, l'Unione ha, invece, trattato i dati personali dei lavoratori in servizio presso il Comando di Polizia locale, mediante la telecamera di videosorveglianza in questione, in assenza di una preliminare VIPD e, pertanto, in violazione dell'art. 35 del Regolamento.

4. Conclusioni.

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

l’archiviazione del presente procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall’art. 11 del Regolamento del Garante n. 1/2019.

Si confermano, pertanto, le valutazioni preliminari dell’Ufficio e si rileva l’illiceità del trattamento di dati personali effettuato dall’Unione, per aver trattato dati personali mediante una telecamera di videosorveglianza, in violazione degli artt. 5, par. 1, lett. a), 6, 12, 13, 35 e 88, par. 1, del Regolamento, nonché 114 del Codice (in relazione all’art. 4, comma 1, della l. n. 300/1970).

Tenuto conto che la violazione delle predette disposizioni ha avuto luogo in conseguenza di un’unica condotta (stesso trattamento o trattamenti tra loro collegati), trova applicazione l’art. 83, par. 3, del Regolamento, ai sensi del quale l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. Considerato che, nel caso di specie, le violazioni più gravi, relative agli artt. 5, par. 1, lett. a), 6, 12, 13 e e 88, par. 1, del Regolamento, nonché 114 del Codice, sono soggette alla sanzione prevista dall’art. 83, par. 5, del Regolamento, come richiamato anche dall’art. 166, comma 2, del Codice, l’importo totale della sanzione è da quantificarsi fino a euro 20.000.000.

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

Ancorché l’Unione abbia dichiarato di aver stipulato un accordo sindacale ai sensi dell’art. 4 della l. 300/1970, di aver provveduto a fornire agli interessati l’informativa sul trattamento dei dati e di aver redatto una VIPD anche con riguardo al trattamento dei dati dei lavoratori, non emerge dalla documentazione in atti che la stessa abbia provveduto anche a modificare il cartello contenente l’informativa di primo livello, apposto in prossimità della telecamera di videosorveglianza oggetto di reclamo, espungendo gli inconferenti riferimenti alle finalità di trattamento connesse alla “sicurezza pubblica – sicurezza urbana – polizia giudiziaria – polizia amministrativa”.

Si rende, pertanto, necessario ingiungere all’Unione, ai sensi dell’art. 58, par. 2, lett. d), del Regolamento, di modificare l’informativa di primo livello sul trattamento dei dati personali, espungendo il riferimento alle finalità di “sicurezza pubblica – sicurezza urbana – polizia giudiziaria – polizia amministrativa” e indicando, invece, le finalità di sicurezza sul lavoro e tutela del patrimonio di cui agli artt. 4, comma 1, della l. 300/1970 e 114 del Codice, espressamente indicate nell’accordo sindacale concluso in data XX.

Ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, l’Unione dovrà provvedere a comunicare a questa Autorità, fornendo un riscontro adeguatamente documentato, entro trenta giorni dalla notifica del presente provvedimento, le iniziative intraprese al fine di dare attuazione a quanto sopra ingiunto ai sensi del citato art. 58, par. 2, lett. d), del Regolamento.

6. Adozione dell’ordinanza ingiunzione per l’applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i e 83 del Regolamento; art. 166, comma 7, del Codice).

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

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

prevista dall'art. 83, par. 5, del Regolamento.

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

Tenuto conto che:

- il trattamento è stato posto in essere in modo non conforme alla disciplina di settore in materia di impiego di strumenti tecnologici sul luogo di lavoro e alle puntuali indicazioni fornite nel tempo dal Garante sia con provvedimenti a carattere generale sia con decisioni su casi specifici, e ha avuto luogo per un esteso arco temporale (da febbraio 2016), interessando, pertanto, un elevato numero di soggetti, ovvero i lavoratori e i visitatori che hanno transitato negli uffici del Comando (art. 83, par. 2, lett. a), del Regolamento);

- le immagini di videosorveglianza non sono state utilizzate nell'ambito del procedimento disciplinare avviato nei confronti del reclamante (art. 83, par. 2, lett. a), del Regolamento);

- la violazione ha carattere colposo (art. 83, par. 2, lett. b), del Regolamento);

- il trattamento non ha riguardato dati particolari appartenenti alle categorie particolari di cui all'art. 9 del Regolamento (cfr. art. 83, par. 2, lett. g), del Regolamento);
  si ritiene che, nel caso di specie, il livello di gravità della violazione commessa dal titolare del trattamento sia alto (cfr. Comitato europeo per la protezione dei dati, "Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR" del 24 maggio 2023, punto 60).

Ciò premesso, nel considerare che il titolare del trattamento è un Ente locale che riunisce Comuni di modeste dimensioni, si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze:

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

- l'Unione ha offerto una buona cooperazione con l'Autorità nel corso dell'istruttoria (art. 83, par. 2, lett. f), 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 (ottomila) per la violazione degli artt. 5, par. 1, lett. a), 6, 12, 13, 35 e 88, par. 1, del Regolamento, nonché 114 del Codice (in relazione all'art. 4, comma 1, della l. n. 300/1970), quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito Internet del Garante. Ciò in considerazione del fatto che il trattamento posto in essere ha avuto ad oggetto dati personali relativi anche a interessati vulnerabili nel contesto lavorativo (cfr. cons. 75 e art. 88 del Regolamento e "Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679", WP 248 del 4 aprile 2017).

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

TUTTO CIÒ PREMESSO IL GARANTE

dichiara, ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, l'illiceità del trattamento effettuato dall'Unione Montana Appennino Parma Est per violazione degli artt. 5, par. 1, lett. a), 6, 12, 13, 35 e 88, par. 1, del Regolamento, nonché 114 del Codice (in relazione all'art. 4, comma 1, della l. n. 300/1970), nei termini di cui in motivazione;

ORDINA

all'Unione Montana Appennino Parma Est, in persona del legale rappresentante pro-tempore, con sede legale in Piazza Giacomo Ferrari, 5 - 43013 Langhirano (PR), C.F. 02706560345, di pagare la somma di euro 8.000 (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 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

- alla predetta Unione, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 8.000 (ottomila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

- alla predetta Unione, ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, di modificare l'informativa di primo livello sul trattamento dei dati personali, espungendo il riferimento alle finalità di "sicurezza pubblica – sicurezza urbana – polizia giudiziaria – polizia amministrativa" e indicando, invece, le finalità di sicurezza sul lavoro e tutela del patrimonio di cui agli artt. 4, comma 1, della l. 300/1970 e 114 del Codice, espressamente indicate nell'accordo sindacale concluso in data XX;

- alla predetta Unione, ai sensi dell'art. 157 del Codice, di comunicare all'Autorità, nel termine di 30 giorni dalla notifica del presente provvedimento, le iniziative intraprese al fine di dare attuazione alle misure imposte; l'eventuale mancato adempimento a quanto ingiunto può comportare l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento;

DISPONE

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

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

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

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

Roma, 10 aprile 2025

IL PRESIDENTE

Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE REGGENTE
Filippi