



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Provvedimento del 12 febbraio 2026 [10226611]

[doc. web n. 10226611]

Provvedimento del 12 febbraio 2026

Registro dei provvedimenti
n. 70 del 12 febbraio 2026

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 dott. Luigi Montuori, segretario generale;

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

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

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

Vista la documentazione in atti;

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

Relatore il dott. Agostino Ghiglia;

PREMESSO

1. Introduzione.

Con reclamo presentato ai sensi dell’art. 77 del Regolamento, il sig. XX, dipendente del Comune di Coccaglio (di seguito, il “Comune”), ha lamentato l’utilizzo di filmati di videosorveglianza a fini disciplinari. In particolare, sarebbero stati mossi degli specifici addebiti all’interessato in relazione a fatti “documentati mediante estrazione ed esibizione delle immagini dell’impianto di

videosorveglianza”.

Ad avviso del reclamante, il Comune avrebbe, inoltre, omesso di fornire un’informativa sul trattamento dei dati personali relativa all’impiego di telecamere di videosorveglianza, non avrebbe stabilito e reso noti i tempi di conservazione dei filmati e non avrebbe esperito le procedure di garanzia previste dall’art. 4 della l. 20 maggio 1970, n. 300 (Statuto dei lavoratori).

2. L’attività istruttoria.

In riscontro a una richiesta d’informazioni rivoltagli dall’Autorità (v. nota prot. n. XX del XX), il Comune, con nota del XX (prot. n. XX), ha dichiarato, in particolare, che:

“il reclamo fa riferimento ad un procedimento disciplinare conclusosi a XX”;

“le telecamere di videosorveglianza del magazzino comunale sono state installate il XX e sono state rese funzionanti dopo alcuni giorni dal momento della loro installazione”;

“il sistema è composto da n. 4 telecamere: due esterne al magazzino comunale che riprendono rispettivamente il lato di ingresso allo stesso magazzino e il lato di deposito merci, mentre la terza telecamera è posizionata internamente al magazzino e riprende la saracinesca e una quarta telecamera che riprende il corsello esterno laterale del magazzino”;

“le telecamere [...] sono state installate [...] per finalità di sicurezza e tutela del patrimonio mobiliare e immobiliare [...], essendosi verificati casi di furto, opportunamente denunciati, di attrezzature depositate nel magazzino in questione”;

“il magazzino [...] è dotato [...] di un impianto di allarme che il giorno XX alle ore XX si è azionato [...]”;

“alle ore 12.15 il [reclamante], contattava la Polizia Locale informando del suo accesso presso i locali del magazzino, da cui ne era derivata l’attivazione dell’allarme, per prelevare un oggetto dal suo armadietto personale [... nonostante] il suo stato di infortunio”;

“[...] sempre nella stessa giornata, il Comandante della Polizia Locale verificava le immagini registrate delle telecamere e ne estraeva i fotogrammi, utili a supportare l’avvio del procedimento disciplinare, che in ogni caso sarebbe stato intrapreso anche in assenza delle immagini, e riportati nella documentazione dello stesso procedimento. Le telecamere presenti presso il magazzino comunale non riprendono né il bagno, né gli spogliatoi e nemmeno l’ufficio”;

“il Comune [...] non ha stipulato un accordo sindacale [...] e non ha richiesto un’autorizzazione dall’Ispettorato Territoriale del Lavoro in relazione all’utilizzo delle telecamere in questione, ai sensi dell’art. 4 della l. 300/1970 poiché l’Ente non ha considerato il magazzino comunale un luogo di lavoro. L’attività lavorativa dell’unico operaio di squadra lavori, [ovvero il reclamante], viene svolta principalmente sul territorio comunale e l’accesso al magazzino comunale, garantito agli operai incaricati dall’Ente avviene solo in casi di necessità per recuperare ovvero depositare i mezzi utili all’espletamento dell’attività che viene svolta sul territorio. Invero [...] l’impianto di videosorveglianza è stato installato per finalità strettamente funzionali alla sicurezza e tutela del patrimonio dell’Ente, senza tuttavia che questo possa implicare un significativo controllo sull’ordinario svolgimento delle attività del personale”;

“il Comune [...] ha previsto una Informativa in merito al trattamento dei dati personali del proprio personale dipendente e collaboratore [...] L’Informativa non è stata redatta ai sensi

dell'art. 4 comma 3 della l. 300/1970 in quanto i dipendenti non sono oggetto di trattamento relativo alla videosorveglianza, se non incidentalmente, come nel caso di specie, il [reclamante]. Per tale trattamento le informazioni di cui all'art. 13 del Regolamento [...] vengono fornite nell'Informativa relativa alla videosorveglianza [...]”;

il Comune ha effettuato una “Valutazione di Impatto sulla protezione dei dati, redatta in relazione all’impiego delle telecamere di videosorveglianza in questione [...] In merito alla Valutazione di Impatto allegata non è stato richiesto parere formale al Responsabile della Protezione dei dati (RPD/DPO) in quanto l’esito della Valutazione effettuata [...] ha registrato un livello di rischio basso per i diritti e le libertà delle persone fisiche, non presentando quindi criticità in ordine alle quali l’Ente avrebbe ritenuto necessario chiedere il supporto o una valutazione delle stesse al RPD”.

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 al Comune, ai sensi dell’art. 166, comma 5, del Codice, l’avvio del procedimento per l’adozione dei provvedimenti di cui all’art. 58, par. 2, del Regolamento, per aver posto in essere un trattamento di dati personali, mediante telecamere di videosorveglianza collocate in luoghi di lavoro, nonché per aver utilizzato i filmati di videosorveglianza a fini disciplinari, in violazione degli artt. 5, par. 1, lett. a) e b), 6, 12, par. 1, 13, 35, 88 del Regolamento, nonché 2-ter e 114 del Codice (in riferimento all’art. 4 della l. 300/1970). 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), il Comune ha presentato una memoria difensiva, dichiarando, in particolare, che:

“l’impianto è stato immediatamente disattivato non appena il titolare ha ricevuto la comunicazione dell’Autorità Garante in data XX”;

“il titolare [...] ha [comunque] sottoscritto in data XX l’accordo con le rappresentanze sindacali ai sensi dell’art. 4 dello Statuto dei Lavoratori (Legge 300/1970); ha realizzato in data XX una valutazione di impatto ai sensi dell’art. 35 del Regolamento [...]; ha esposto la nuova informativa di primo livello (Cartello) nelle zone videosorvegliate; ha consegnato a tutti i dipendenti/collaboratori la nuova informativa dettagliata ai sensi dell’art. 13 del Regolamento [...]”.

3. Esito dell’attività istruttoria.

3.1 La liceità del trattamento.

Il trattamento di dati personali relativi a lavoratori, mediante telecamere di videosorveglianza idonee a riprendere anche il personale che transita o sosta nei luoghi di lavoro, può essere effettuato dal datore di lavoro se esso è necessario 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” (88, par. 2, del Regolamento, a cui fa rinvio l’art. 6, par. 2, del Regolamento).

Come costantemente ribadito nei provvedimenti del Garante, i trattamenti conseguenti all’impiego degli strumenti tecnologici nei luoghi ove si svolge anche l’attività lavorativa, trovano la propria base giuridica nella disciplina di settore di cui all’art. 4 della l. n. 300/1970 (Statuto dei Lavoratori),

il cui comma 1 prevede 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”.

Tale disposizione perimetra in modo uniforme a livello nazionale l'ambito del trattamento consentito in ogni contesto lavorativo (pubblico e privato) e costituisce nell'ordinamento interno una disposizione più specifica e di maggiore garanzia di cui all'art. 88 del Regolamento, la cui osservanza - 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”) - è condizione di liceità del trattamento (v. art. 5, par.1, lett. a) e 6, par. 1, lett. c) del Regolamento; v., a livello europeo, le indicazioni contenute nelle “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, 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; cfr. par. 4.1 del “Provvedimento in materia di videosorveglianza” dell'8 aprile 2010, doc. web n. 1712680, e, 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, tra cui, con specifico riguardo al ricorso alla videosorveglianza sui luoghi di lavoro, provv.ti 23 ottobre 2025, n. 628, doc. web n. 10196164; 10 luglio 2025, n. 410, doc. web n. 10162731; 10 aprile 2025, n. 201, doc. web n. 10139433; 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).

Ciò in conformità alla giurisprudenza della Corte europea dei diritti dell'uomo, nel caso *Antovic e Mirkovic v. Montenegro* (Application n. 70838/13 del 28.11.2017), che ha stabilito che il rispetto della vita privata deve essere esteso anche ai luoghi di lavoro pubblici, evidenziando che l'impiego di dispositivi video sul posto di lavoro può essere giustificato 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.

Nel caso di specie, risulta accertato che il Comune, a partire dal mese di XX ha installato e messo in funzione quattro telecamere di videosorveglianza che riprendono l'interno e l'esterno di un magazzino comunale per finalità di “sicurezza e tutela del patrimonio”. Ciò senza previamente esperire le procedure di garanzie di cui all'art. 4 della l. 300/1970, non avendo il Comune considerato il magazzino in questione quale un luogo di lavoro, sul presupposto che “l'accesso al magazzino comunale, garantito agli operai incaricati dall'Ente avviene solo in casi di necessità per recuperare ovvero depositare i mezzi utili all'espletamento dell'attività che viene svolta sul territorio”.

Occorre, a tal riguardo, evidenziare che le pur legittime esigenze di tutela del patrimonio dell'Ente, invocate dallo stesso, 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 di liceità del relativo trattamento.

Come anche recentemente ribadito dal Garante (v. provv. 13 marzo 2025, n. 135, doc. web n.

10128005), anche a seguito delle modifiche apportate alla l. 20 maggio 1970, n. 300 dall'art. 23 del d. lgs. 14 settembre 2015, n. 151, il datore di lavoro può impiegare strumenti tecnologici, inclusi impianti di videosorveglianza, soltanto per perseguire le finalità riconducibili a quelle tassativamente selezionate dal legislatore ("organizzative e produttive", "di sicurezza del lavoro" e "di tutela del patrimonio aziendale"), atteso che il controllo a distanza dell'attività lavorativa è consentito dalla legge, nel rispetto delle condizioni di garanzia ivi previste, solo incidentalmente, ossia in occasione del perseguimento di tali legittime finalità, così assumendo un carattere tipicamente indiretto e preterintenzionale.

Per tali ragioni, non rileva quanto dichiarato dal titolare del trattamento in merito alla circostanza che l'Ente non ha ritenuto necessario né stipulare un accordo sindacale né informare i dipendenti in merito all'impiego del sistema di videosorveglianza, sul presupposto che essi "non sono oggetto di trattamento relativo alla videosorveglianza, se non incidentalmente", tale affermazione confermando - stante il perdurante divieto di controllo diretto sull'attività dei lavoratori (cfr. Cass. pen., 8 maggio 2017, n. 22148/2017, nella parte in cui richiama l'orientamento, "pienamente valido anche a seguito della novella di cui al d.lg. 14 settembre 2015, n. 151, art. 23", in base al quale "le apparecchiature finalizzate al mero controllo a distanza della prestazione lavorativa [debbono essere] assolutamente vietate [...per] contrasto con i principi della Costituzione"; v. anche Cass. civ., 14 maggio 2021, n. 25732) - che il trattamento in questione avesse proprio quel carattere indiretto e preterintenzionale, ammesso dunque dall'ordinamento, ma esclusivamente in presenza delle garanzie procedurali previste dalla legge (art. 4, comma 1, della l. n. 300/1970 e art. 114 del Codice).

D'altra parte, il sistema di protezione dei dati, integrato con l'art. 4 della l. n. 300/1970, tutela la persona che lavora non solo quando i dispositivi di sorveglianza siano posti all'interno dei locali di lavoro - essendo irrilevante la circostanza che l'accesso a detti locali da parte dei lavoratori avvenga in maniera discontinua e per brevi archi temporali - ma anche nel caso in cui siano sottoposte a videosorveglianza aree di pertinenza della sede datoriale, anche esterne o perimetrali, in cui comunque transitano i lavoratori, stante la possibilità, come nel caso di specie, di riprendere la loro immagine e le attività da essi svolte (cfr. provv. ti 23 ottobre 2025, n. 628, cit., relativo all'impiego di una telecamera collocata sulla pubblica via per finalità di sicurezza urbana e inquadrante l'ingresso della casa comunale utilizzato anche dai dipendenti; 10 aprile 2025, n. 201, cit., sull'impiego di una telecamera di videosorveglianza inquadrante l'ingresso esterno di una sede di Polizia locale e parte del parcheggio delle auto di servizio; 11 marzo 2021, n. 90, doc. web n. 9582791, riguardante l'impiego di telecamere di videosorveglianza nei corridoi di un edificio ospitante un Dipartimento di un Ateneo; 9 maggio 2018, n. 277, doc. web n. 8998303, riguardante un sistema di videosorveglianza installato in aree interne ed aree esterne a un edificio della sede di un ente pubblico, inclusi gli accessi; 18 aprile 2013, n. 200, doc. web n. 2483269, riguardante le riprese che interessavano in particolare gli accessi, i corridoi e alcuni ambienti aperti all'utenza di un Archivio di Stato; 9 febbraio 2012, n. 56, doc. web n. 1886999, nel quale le riprese riguardavano gli accessi ai garage di un Comando di polizia locale, nonché il corridoio interno di accesso ai locali dell'armeria; 17 novembre 2011, n. 434, doc. web n. 1859558, nel quale le riprese interessavano gli ingressi principali e di emergenza, i corridoi posti ai diversi piani, nonché le aree di accesso a talune zone degli uffici).

L'Ente ha, invece, nel caso di specie, attivato le telecamere di videosorveglianza, sia all'interno che all'esterno dei locali adibiti a magazzino, senza assicurare il rispetto delle garanzie previste dalla disciplina lavoristica e di protezione dei dati a tutela di lavoratori.

Alla luce delle considerazioni che precedono, deve concludersi che il trattamento dei dati personali del reclamante e degli altri lavoratori autorizzati all'accesso al magazzino o che comunque hanno transitato nei pressi dello stesso è stato posto in essere dall'Ente in maniera non conforme al principio di "liceità, correttezza e trasparenza", nonché in assenza di un idoneo presupposto di liceità, in violazione degli artt. 5, par. 1, lett. a), 6, par. 1, lett. c) e parr. 2 e 3, e 88

del Regolamento, e 2-ter e 114 del Codice (in riferimento all'art. 4 della l. n. 300/1970).

3.2 L'utilizzo di filmati di videosorveglianza nel contesto del rapporto di lavoro per fini disciplinari.

Il Comune ha, altresì, utilizzato i filmati di videosorveglianza, ottenuti dalle telecamere in questione, per formulare talune contestazioni disciplinari nei confronti del reclamante (v. la contestazione disciplinare del XX in atti, ove si legge che "i fatti sopra circostanziati sono stati documentati mediante estrazione ed esibizione delle immagini di videosorveglianza").

Nel ribadire che i trattamenti di dati personali connessi all'impiego di strumenti dai quali possa derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori devono essere svolti nel rigoroso rispetto dei limiti e delle condizioni previste dalla cornice legislativa di riferimento, che ne costituisce, come detto, la base giuridica, si osserva quanto segue.

Come più volte evidenziato dal Garante, anche le esigenze di tutela del patrimonio datoriale sono state espressamente incluse dal legislatore tra le sole finalità lecite perseguibili mediante sistemi che possono comportare il controllo indiretto sulla generalità dei dipendenti, subordinandone l'installazione e l'utilizzazione all'accordo sindacale o, in alternativa, all'autorizzazione pubblica, con la conseguenza che, qualora non vengano rispettate tali condizioni per il lecito impiego dei predetti sistemi, qualunque trattamento, anche ulteriore, di tali dati, inclusa la loro "estrazione, consultazione e uso" (art. 4, par. 1, n. 1), del Regolamento), debba considerarsi non conforme ai principi di "liceità, correttezza e trasparenza" e "limitazione della finalità", sprovvisto di idonea base giuridica e quindi illecito (cfr., tra i tanti, provv. 1° dicembre 2022, n. 409, doc. web n. 9833530). Conseguentemente, i trattamenti di dati personali effettuati mediante sistemi di videosorveglianza sull'attività dei lavoratori, posti in essere in assenza delle predette garanzie, si pongono al di fuori del quadro di liceità delineato dalle disposizioni di settore e dalla disciplina in materia di protezione dei dati.

Più nel dettaglio e con specifico riguardo al caso di specie, la predetta disciplina di settore consente inoltre di utilizzare, per ulteriori finalità nell'ambito della gestione del rapporto, solo le informazioni già lecitamente raccolte nel rispetto delle condizioni e dei limiti previsti dall'art. 4 della l. n. 300/1970 e, dunque, nei limiti in cui l'originaria raccolta sia stata lecitamente effettuata. Tale quadro presuppone quindi un'autonoma determinazione del titolare circa l'utilizzazione delle informazioni, ove già lecitamente raccolte nel rispetto delle condizioni e dei limiti previsti dall'art. 4, commi 1 o 2 della l. n. 300/70, anche per ulteriori trattamenti necessari alla gestione del rapporto di lavoro (art. 4, comma 3, della l. n. 300/1970). Tali successive ed eventuali operazioni di trattamento presuppongono il rispetto del quadro normativo di riferimento in materia sia di controlli a distanza dei lavoratori (ai sensi dei commi 1 e 2) sia di protezione dei dati. Ciò anche con riguardo alla necessità di fornire ai lavoratori ogni necessaria informazione per assicurare agli stessi piena consapevolezza degli ulteriori trattamenti che il datore di lavoro si riserva di effettuare (sul punto, v., tra i tanti, provv. 23 ottobre 2025, n. 628, cit.; 11 aprile 2024, n. 234, cit.; 1° dicembre 2022, n. 409, cit.; 28 ottobre 2021, n. 384, doc. web n. 9722661; 13 maggio 2021, n. 190, doc. web n. 9669974; cfr. anche il "Documento di indirizzo "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati"", adottato con provv. 6 giugno 2024, n. 364, doc. web n. 10026277, par. 4.1).

Nel caso di specie, non avendo il Comune osservato le garanzie previste dall'art. 4, comma 1, della l. 300/1970 e fornito ai lavoratori alcuna informativa in merito alla possibilità che il sistema di videosorveglianza avrebbe potuto essere impiegato anche a fini disciplinari, deve concludersi che il trattamento, da parte dell'Ente, di dati raccolti mediante tale sistema, nell'ambito del procedimento disciplinare avviato nei confronti del reclamante, è avvenuto in maniera non conforme tanto alla disciplina di settore in materia di controlli a distanza quanto alla disciplina in materia di protezione dei dati, 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, comma 3, della l. n. 300 del 1970.

3.3. La trasparenza nei confronti degli interessati.

Nel rispetto del principio di “liceità, correttezza e trasparenza” (art. 5, par. 1, lett. a), del Regolamento), il titolare del trattamento deve adottare misure appropriate per fornire all'interessato tutte le informazioni di cui agli artt. 13 e 14 del Regolamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (cfr. art. 12, par. 1, del Regolamento).

Il Comune ha, a tal riguardo, dichiarato di aver fornito ai propri dipendenti un'informativa sul trattamento dei dati personali che, tuttavia, “non è stata redatta ai sensi dell'art. 4 comma 3 della l. 300/1970 in quanto i dipendenti non sono oggetto di trattamento relativo alla videosorveglianza”.

Stante quanto sopra evidenziato in relazione alla riconducibilità agli artt. 114 del Codice e 4 della l. n. 300/1970 dei trattamenti di dati personali posti in essere mediante i dispositivi di videosorveglianza installati all'interno e all'esterno del magazzino in questione, il Comune avrebbe, invece, dovuto fornire ai propri lavoratori una specifica informativa sul trattamento dei dati personali nell'ambito di tale attività di videosorveglianza per il perseguimento della finalità di “tutela del patrimonio aziendale” di cui all'art. 4, comma 1, della l. 300/1970. Tale informativa era, peraltro, comunque dovuta, indipendentemente dalla riserva da parte del datore di lavoro di utilizzare le immagini di videosorveglianza anche a tutti i fini connessi al rapporto di lavoro, come previsto dall'art. 4, comma 3, della l. n. 300/1970.

Deve, pertanto, concludersi che l'Ente ha effettuato un trattamento di dati personali, mediante dispositivi video attivati sul luogo di lavoro, in maniera non conforme al principio di “liceità, correttezza e trasparenza”, in violazione degli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento.

3.4. La valutazione di impatto sulla protezione dei dati.

Quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche e, in ogni caso, al ricorrere delle ipotesi tassativamente previste, il titolare del trattamento, prima di porre in essere lo stesso, deve svolgere una valutazione di impatto sulla protezione dei dati, al fine di adottare, in particolare, le misure adeguate ad affrontare tali rischi, consultando preventivamente il Garante, ove ne ricorrano i presupposti (v. artt. 35 e 36, par. 1, del Regolamento).

Tenuto conto delle indicazioni fornite anche a livello europeo sul punto, si ritiene che, nel caso specie, l'Ente avrebbe dovuto svolgere una valutazione di impatto sulla protezione dei dati prima di avviare il trattamento, atteso che lo stesso comporta rischi specifici per i diritti e le libertà dei lavoratori. Ciò, 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”) quanto del fatto che sono impiegati sistemi che comportano il “monitoraggio sistematico” in ambito lavorativo, 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; v. 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; 13 maggio 2021, n. 190, cit.). La mancata esecuzione di una valutazione di impatto sulla protezione dei dati in relazione a sistemi di videosorveglianza impiegati nel contesto lavorativo è stata, per tali motivi, oggetto di recenti provvedimenti anche correttivi e sanzionatori del Garante

(v. in particolare, provv.ti 23 ottobre 2025, n. 628, cit.; 10 luglio 2025, n. 410, doc. web n. 10162731; 10 aprile 2025, doc. web n. 10139433; 13 marzo 2025, n.135, doc. web n. 10128005; 16 novembre 2023, n. 578, doc. web n. 9963486).

Il Comune non ha, invece, comprovato di aver svolto una valutazione di impatto sulla protezione dei dati prima di dare avvio alle attività di videosorveglianza all'interno e all'esterno del magazzino in questione. L'Ente ha, infatti, depositato in atti una valutazione di impatto sulla protezione dei dati priva non solo di data certa ma anche di meri riferimenti temporali, nonché di firma del legale rappresentante dell'Ente o di altro soggetto da questi autorizzato. Tale documento fa, peraltro, erroneamente riferimento agli "Art.6.1, lettera e) [...]" e "Art.9.2, lettera g)" del Regolamento quali basi giuridiche del trattamento in questione, non essendo stata, pertanto, effettuata una corretta "descrizione sistematica dei trattamenti previsti e delle finalità del trattamento" (art. 35, par. 7, lett. a), del Regolamento).

Quanto alla circostanza che il Comune non avrebbe acquisito il parere del proprio Responsabile della protezione dei dati (RPD) ai fini dello svolgimento della valutazione di impatto, sul presupposto che "l'esito della valutazione effettuata [dal] Comune ha registrato un livello di rischio basso per i diritti e le libertà delle persone fisiche", deve farsi presente che, ai sensi dell'art. 35, par. 2, del Regolamento, "il titolare del trattamento, allorché svolge una valutazione di impatto sulla protezione dei dati, si consulta con il [RPD], qualora ne sia designato uno" (v. anche art. 39, par. 1, lett. c), del Regolamento, ai sensi del quale "il [RPD] è incaricato almeno dei seguenti compiti: : [...] fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35").

Come evidenziato a livello europeo nelle "Linee guida in materia di valutazione di impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679", adottate il 4 ottobre 2017 dal Gruppo di lavoro art. 29 e fatte proprie dal Comitato europeo per la protezione dei dati con Endorsement 1/2018 del 25 maggio 2018, "il titolare del trattamento deve consultarsi con il [...] RPD [...], qualora ne sia designato uno (articolo 35, paragrafo 2) e il parere ricevuto, così come le decisioni prese dal titolare del trattamento, de[vono] essere documentate all'interno della valutazione di impatto sulla protezione dei dati" (pag. 17).

Pertanto, sia il parere del RPD sia le decisioni prese dal titolare anche alla luce di tale parere devono costituire parte integrante della valutazione di impatto, ben potendo il RPD non concordare con le valutazioni effettuate dal titolare del trattamento ed esprimere un diverso avviso.

Non risulta, pertanto, conforme al sistema di protezione dei dati delineato dal Regolamento, né corretto sul piano metodologico, il mancato coinvolgimento del RPD da parte del Comune in fase di redazione della valutazione di impatto sulla protezione dei dati, essendo del tutto irrilevante a tal riguardo che, all'esito della stessa, non sia risultato, ad avviso dell'Ente, un rischio residuale elevato per i diritti e le libertà degli interessati.

Alla luce di tutte le considerazioni che precedono, deve concludersi che il Comune ha posto in essere un trattamento di dati personali dei lavoratori, mediante il sistema di videosorveglianza in questione, in assenza di una preliminare valutazione di impatto sulla protezione dei dati 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

rilevi 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 dal Comune, per aver posto in essere un trattamento di dati personali mediante dispositivi video, utilizzando anche i filmati a fini disciplinari, in violazione degli artt. 5, par. 1, lett. a) e b), 6, par. 1, lett. c) e parr. 2 e 3, 12, par. 1, 13, 35, 88 del Regolamento, nonché 2-ter e 114 del Codice (in riferimento all'art. 4 della l. 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) e b), 6, 12, par. 1, 13, e 88 del Regolamento, e 2-ter e 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.

In tale quadro, considerando, in ogni caso, che la condotta ha esaurito i suoi effetti - atteso che il Comune ha dichiarato di aver disattivato il sistema di videosorveglianza e di aver cessato ogni attività di trattamento dei dati personali oggetto della violazione - non ricorrono i presupposti per l'adozione di ulteriori misure correttive di cui all'art. 58, par. 2, del Regolamento.

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

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

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

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

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 maggio XX a giugno XX), interessando i lavoratori che in tale periodo, ancorché occasionalmente, hanno transitato all'interno o nei pressi del magazzino sottoposto a videosorveglianza (cfr. art. 83, par. 2, lett. a), del Regolamento);

la violazione ha carattere colposo (cfr. 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 Comune di modeste dimensioni (circa 8.800 abitanti), si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze:

non risultano precedenti violazioni pertinenti commesse dal titolare del trattamento (cfr. art. 83, par. 2, lett. e), del Regolamento);

il Comune ha offerto una buona cooperazione con l'Autorità nel corso dell'istruttoria, avendo, peraltro, provveduto a disattivare le telecamere di videosorveglianza in questione non ha appena ha ricevuto la contestazione di violazione amministrativa, avendo provveduto, in particolare, a stipulare un accordo sindacale in relazione ai futuri trattamenti (cfr. 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 6.000 (seimila) per la violazione degli artt. 5, par. 1, lett. a) e b), 6, par. 1, lett. c) e parr. 2 e 3, 12, par. 1, 13, 35, 88 del Regolamento, nonché 2-ter e 114 del Codice (in riferimento all'art. 4 della l. 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 a interessati vulnerabili nel contesto lavorativo.

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

TUTTO CIÒ PREMESSO IL GARANTE

dichiara, ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, l'illiceità del trattamento effettuato dal Comune di Coccaglio per la violazione degli artt. 5, par. 1, lett. a) e b), 6, par. 1, lett. c) e parr. 2 e 3, 12, par. 1, 13, 35, 88 del Regolamento, nonché 2-ter e 114 del Codice, nei termini di cui in motivazione;

ORDINA

al Comune di Coccaglio, in persona del legale rappresentante pro-tempore, con sede legale in Via Matteotti, 10 - 25030 Coccaglio (BS), C.F. 00821390176, di pagare la somma di euro 6.000 (seimila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione. Si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

al predetto Comune, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 6.000 (seimila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

DISPONE

- ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, la pubblicazione dell'ordinanza ingiunzione sul sito internet del Garante;
- ai sensi dell'art. 154-bis, comma 3 del Codice e dell'art. 37 del Regolamento del Garante n. 1/2019, la pubblicazione del presente provvedimento sul sito internet dell'Autorità;
- ai sensi dell'art. 17 del Regolamento del Garante n. 1/2019, l'annotazione delle violazioni e delle misure adottate in conformità all'art. 58, par. 2 del Regolamento, nel registro interno dell'Autorità previsto dall'art. 57, par. 1, lett. u) del Regolamento.

Ai sensi degli artt. 78 del Regolamento, 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento è possibile proporre ricorso dinanzi 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, 12 febbraio 2026

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Montuori