



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

## **Provvedimento dell'11 aprile 2024 [10013356]**

**VEDI ANCHE [Newsletter del 21 maggio 2024](#)**

[doc. web n. 10013356]

### **Provvedimento dell'11 aprile 2024**

Registro dei provvedimenti  
n. 234 dell'11 aprile 2024

#### **IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

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

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

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

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

Vista la documentazione in atti;

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

Relatore l'avv. Guido Scorza;

#### **PREMESSO**

##### **1. Introduzione.**

Con segnalazione presentata ai sensi dell'art. 144 del Codice dalla Sig.ra XX, dipendente del Comune di Madignano (di seguito, il "Comune"), è stata lamentata l'installazione di un sistema di

videosorveglianza nella sede del Comune, in prossimità dei sistemi di rilevazione delle presenze e in assenza dell'accordo con le organizzazioni sindacali, nonché l'impiego di tale sistema per l'effettuazione di specifiche contestazioni disciplinari alla dipendente in ordine al mancato rispetto dell'orario di servizio e alla violazione dei propri doveri d'ufficio.

## **2. L'attività istruttoria.**

In riscontro a una richiesta d'informazioni dell'Autorità (v. nota prot. n. XX del XX), il Comune, con nota dell'XX (prot. n. XX, acquisita al protocollo del Garante n. XX del XX), ha dichiarato, in particolare, che:

“a seguito di comportamenti non conformi al rispetto del contratto di lavoro, è stata emessa una contestazione disciplinare ad una dipendente del Comune [...], in ordine al mancato rispetto dell'orario di servizio; le prime segnalazioni riguardanti la condotta della dipendente erano state riportate al Sindaco da alcuni cittadini [...]”;

“nel corso dell'indagine interna, tali segnalazioni sono state confrontate con le timbrature riportate nei cartellini di rilevazione delle presenze mensili”;

“le informazioni acquisite [sono] state rilevate da supporto cartaceo, prodotto dall'orologio-timbratore quale unico strumento utilizzato per la rilevazione dell'orario di servizio dei dipendenti”;

“la telecamera posizionata all'interno dell'atrio del comune è stata installata al solo scopo di tutelare il patrimonio comunale e l'incolumità dei dipendenti [...]”;

“il sistema di videosorveglianza attualmente in funzione è stato autorizzato dall'Ispettorato del lavoro di Cremona con Provvedimento n. XX”;

“fin dalla sua installazione [...] risulta volontariamente oscurato il riquadro in alto a destra, al fine di non riprendere la zona dove sono ubicati i rilevatori di presenza, nel rispetto delle normative vigenti”.

In riscontro a un'ulteriore richiesta d'informazioni dell'Autorità (v. nota prot. XX del XX), il Comune, con nota del XX (prot. n. XX, acquisita al protocollo del Garante n. XX del XX), ha dichiarato, in particolare, che:

“per quanto riguarda la data di installazione del sistema di sorveglianza nell'atrio del Comune, non [si è] riusciti a risalire ad una data precisa”;

“la telecamera è stata fisicamente posizionata tra i mesi di XXe XX”;

“il collegamento all'impianto di videosorveglianza è avvenuto nel mese di XX, a seguito di un'aggressione nei confronti dell'assistente sociale e dell'allora assessore avvenuta verso la fine del mese di XX”;

“a far data da allora, non essendoci stati ulteriori eventi violenti, la videocamera in questione non è stata oggetto di controlli specifici”.

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:

- omesso di fornire agli interessati (ovvero sia i lavoratori sia i visitatori presso la sede del

Comune) un'informativa sul trattamento dei dati personali mediante il predetto sistema di videosorveglianza, in violazione degli artt. 5, par. 1, lett. a), 12 e 13 del Regolamento;

- trattato dati personali mediante il predetto sistema di videosorveglianza in assenza delle condizioni previste dalla disciplina in materia di controlli a distanza, in violazione degli artt. 5, par. 1, lett. a), 6, e 88 del Regolamento, nonché 114 del Codice, in riferimento all'art. 4, comma 1, della l. n. 300 del 1970;

- utilizzato i dati raccolti mediante il predetto sistema di videosorveglianza nell'ambito del procedimento disciplinare avviato nei confronti dell'interessata, in assenza dei presupposti richiesti dalla disciplina di settore in materia di controlli a distanza, 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.

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, dalla l. 24 novembre 1981, n. 689).

Con nota del XX (prot. n. XX), il Comune, che non ha chiesto di essere audito, ha presentato una memoria difensiva, dichiarando, in particolare, che:

la finalità del trattamento non consisteva nella "videosorveglianza sui luoghi di lavoro per la tutela del patrimonio aziendale", bensì nella "pubblica sicurezza e [...] accertamento dei reati", così come previsto dal "regolamento approvato con delibera n. 26 del 29/06/2005", ai sensi del quale il Comune può "monitorare, anche con l'uso di videocamere, il territorio, l'interno e l'esterno degli edifici pubblici (art. 2, n. 5)";

"ulteriore prova del perseguimento delle sole finalità di Pubblica Sicurezza e di accertamento dei reati, risiede nel fatto che l'unico monitor per la visualizzazione delle immagini è posizionato nell'ufficio della Polizia Locale adiacente all'atrio di ingresso del Municipio dov'è collocata la videocamera interna, senza che il Sindaco possa tenere monitorate costantemente le immagini";

"non è stata mai prevista [dal] Comune, installata o collegata alcuna videocamera che sia in grado di riprendere, in alcun modo, i lavoratori dipendenti del Comune non solo negli Uffici posti, peraltro, al piano superiore rispetto all'unica telecamera interna [...], ma nemmeno nelle immediate adiacenze degli stessi e, tantomeno, in altri ambienti dove possa dirsi lesa la loro dignità o la loro riservatezza. L'unica telecamera interna all'edificio è indirizzata nell'atrio di entrata del pubblico";

il Comune ha "disposto [...] il collegamento della videocamera "a seguito di una aggressione subita dall'assistente sociale";

"è evidente che l'unico scopo perseguito [dal Comune], così come dalle precedenti, è la tutela della Sicurezza collettiva, la prevenzione e l'accertamento dei reati e non la videosorveglianza sui luoghi di lavoro per la tutela del patrimonio aziendale. Gli interessati al trattamento, quindi, non sono mai stati i dipendenti pubblici del Comune in quanto tali ma la collettività tutta";

"va da sé, pertanto, che [...] non è applicabile la L. n. 300/1970";

"coerentemente con [tali] reali finalità del trattamento [...], il] Sindaco, quale Ufficiale di Polizia Giudiziaria ex art. 57, comma 1 lett. c c.p.p., all'esito dei gravi indizi a carico della segnalante consistiti nel mancato adempimento delle "formalità previste per la rilevazione delle presenze" [...] e nelle lamentele "da parte del restante personale", nonché, nelle

“segnalazioni riguardanti la condotta della dipendente riportate al Sindaco da alcuni cittadini, che stazionando quotidianamente nei pressi del Comune, avevano notato e riferito con dovizia di particolari, gli accadimenti riportati nel procedimento” [...] decideva, per il tempo strettamente necessario, di trattare il dato raccolto nel rispetto delle finalità esplicate nel regolamento comunale [sulla videosorveglianza]”;

“è di tutta evidenza la piena legittimità dell’originaria raccolta e, di conseguenza, dell’utilizzo del dato atteso che nel corso delle indagini di P.G. la condotta non ricade nell’ambito del [Regolamento] ma nel d.lgs. 51/2018 inerente il trattamento dei dati effettuato dalle Autorità Pubbliche a fini di prevenzione, indagine, accertamento o perseguimento degli illeciti. [...] Accertamento che, nella specie, riguardava condotte post[e] in essere dalla segnalante ed aventi rilievo penale e, di conseguenza, portate anche all’attenzione degli inquirenti a mezzo di querela orale sporta in data XX”;

“nella denegata ipotesi in cui si ritenga che nel trattamento dei dati [...] [il Comune] sia qualificabile come datore di lavoro, l’ormai costante dettato giurisprudenziale al riguardo legittimerebbe comunque la condotta [del Comune] [...]”;

“[il Sindaco del Comune], infatti, sulla base dell’emersione di concreti indizi tali da segnalare la presenza di illeciti in atto da parte della dipendente [...] risalenti ad un periodo precedente al collegamento della videocamera interna - “dall’anno XX” [...] - avvenuto nel XX, non effettuava un controllo diretto a monitorare costantemente il lavoratore dipendente in prossimità dello stesso come richiesto nella fattispecie dei controlli a distanza; anche perché sarebbe stato impossibile, a fronte del posizionamento della videocamera posta, si ribadisce, al piano inferiore rispetto a dove si esercita l’attività lavorativa [...]”;

“in realtà, la condotta de quo era, invece, diretta ad accertare specifiche condotte illecite lesive dell’immagine dell’Ente [...]”;

“quindi, i dati sono stati trattati in conseguenza di quei “controlli difensivi in senso stretto” che la giurisprudenza maggioritaria ha già sancito essere estranei dal campo di applicazione dell’art. 4 dello Statuto dei lavoratori [...] ([v.] tra le altre, Cass. sezione lavoro n. 25732/2021; Cass. pen. 3255/2021, in linea con quanto deciso dalla CEDU nella sentenza 17/10/2019 caso Lopez Ribalda e altri V Spagna in tema di videosorveglianza occulta)”;

per quanto attiene alla trasparenza del trattamento, il predetto regolamento comunale “riporta [...] tutte le informazioni di cui all’art. 13 del [Regolamento]”;

tale regolamento è “dalla sua approvazione accessibile a chiunque (art. 22) [...] mediante messa a disposizione al pubblico, qualora ne faccia richiesta”;

“dunque, unitamente alla cartellonistica presente nelle immediate vicinanze delle videocamere dislocate (art. 2, n.5 del regolamento comunale), gli interessati sono in grado di ricevere tutte le informazioni previste dall’art. 13, comma 1 del [...] Regolamento [...], attraverso un’informativa rappresentata appunto da detto regolamento comunale disponibile, peraltro, anche sul sito web del Comune”;

quali “fattori attenuanti applicabili alle circostanze del caso [...] si p[uò] tenere in considerazione la bassa soglia inerente [al] grado di protezione della privacy dei dipendenti (sentenza 17/10/2019 caso Lopez Ribalda e altri V Spagna), del tutto equiparabile a quella del pubblico che accede quotidianamente all’interno del Comune”;

“in secondo luogo, si consideri che l’Amministrazione ha agito tempestivamente disattivando la telecamera in occasione dell’accesso Ispettivo dell’Ispettorato del lavoro e riattivandola solo successivamente all’ottenimento del Provvedimento n. XX di autorizzazione all’utilizzo

dell'impianto".

### **3. Esito dell'attività istruttoria.**

#### **3.1. La normativa in materia di protezione dei dati.**

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. sez. 3.2 delle "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video" del Comitato europeo per la protezione dei dati del 29 gennaio 2020).

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 può essere effettuato, dal titolare in qualità di datore di lavoro, se è necessario, in generale, per la gestione del rapporto di lavoro e nell'ambito del quadro giuridico applicabile definito da leggi, dalla normativa comunitaria, da regolamenti o da contratti collettivi (artt. 6, par. 1, lett. c), e 88 del Regolamento). In tale quadro, il datore di lavoro deve, quindi, 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 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 recente FAQ del Garante n. 9 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, della l. 20 maggio 1970, n. 300 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".

Il comma terzo del medesimo articolo precisa poi che "le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal [Codice]".

La normativa europea prevede che i dati personali devono essere trattati "in modo lecito, corretto

e trasparente nei confronti dell'interessato" e "raccolti per finalità determinate, esplicite e legittime" (principi di "liceità, correttezza e trasparenza" e "limitazione della finalità"), ammettendo la possibilità di successivi trattamenti ma solo "in modo che non sia incompatibile con [le] finalità" iniziali del trattamento (art. 5, par. 1, lett. a) e b), del Regolamento).

In tale quadro, il titolare può utilizzare per ulteriori trattamenti i soli dati personali lecitamente raccolti in presenza di un'idonea base giuridica, avendo previamente "soddisfatto tutti i requisiti per la liceità del trattamento originario" (cfr. cons. n. 50 del Regolamento), e dunque nei limiti in cui l'originaria raccolta sia stata lecitamente effettuata, avuto riguardo alla finalità principale e nel rispetto dei principi generali di protezione dei dati, tra cui quello di "liceità, correttezza e trasparenza", in attuazione del quale 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).

### **3.2. La liceità e la trasparenza del trattamento dei dati personali dei lavoratori mediante il sistema di videosorveglianza.**

Sulla base degli elementi acquisiti e dei fatti emersi a seguito dell'attività istruttoria, risulta accertato che, tra i mesi di XX e XX, il Comune ha installato una telecamera di videosorveglianza nell'atrio della propria sede, collegando la stessa all'impianto di videosorveglianza nel mese di XX, a seguito di un'aggressione subita da un'assistente sociale e da un assessore.

L'installazione di tale telecamera è stata, tuttavia, autorizzata dall'Ispettorato territoriale del lavoro di Cremona con provvedimento n. XX soltanto in data XX (v. all. 1 alla nota prot. n. XX del XX).

Ciò premesso, deve osservarsi che, per quanto attiene alle finalità di trattamento perseguita mediante tale telecamera di videosorveglianza, il Comune, nel corso dell'istruttoria e nelle proprie memorie difensive, ha sostenuto tesi tra loro eterogenee e in reciproca contraddizione.

In un primo momento, il Comune ha, infatti, affermato che la telecamera in questione sarebbe stata installata "al solo scopo di tutelare il patrimonio comunale e l'incolumità dei dipendenti" (v. dell'XX, prot. n. XX).

Successivamente, in sede di memoria difensiva, il Comune ha sostenuto la tesi per cui l'unica finalità di trattamento perseguita sarebbe stata, in realtà, di "pubblica sicurezza e [...] accertamento dei reati".

Al riguardo, deve osservarsi che non vi è alcuna evidenza in atti che la telecamera in questione fosse stata installata dal Comune per il perseguimento di finalità di sicurezza urbana. Ai sensi dell'art. 5, co. 2, lett. a), del d.l. 20 febbraio 2017, n. 14, i Comuni possono, infatti, installare telecamere di videosorveglianza sulla pubblica via per il perseguimento degli obiettivi di "prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria", previa stipula di un patto per l'attuazione della sicurezza urbana con la Prefettura territorialmente competente. Nel caso di specie - posto che la predetta telecamera era idonea a riprendere anche gli ambienti interni della sede del Comune, 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 - il Comune non ha comunque comprovato di aver stipulato con la Prefettura territorialmente un patto per l'attuazione della sicurezza urbana che espressamente prevedesse l'installazione della telecamera in questione all'interno dell'atrio della sede del Comune per il perseguimento di finalità connesse alla sicurezza urbana.

Né l'impiego della telecamera in questione può ricondursi al più ampio ambito della pubblica sicurezza, atteso che la Polizia locale non ha competenze di carattere generale in tale materia.

L'art. 5, comma 1, lett. c), della l. 7 marzo 1986, n. 65 ("Legge-quadro sull'ordinamento della polizia municipale"), prevede, infatti, che "il personale che svolge servizio di polizia municipale, nell'ambito territoriale dell'ente di appartenenza e nei limiti delle proprie attribuzioni, esercita anche [...] funzioni ausiliarie di pubblica sicurezza"; ciò "collaboran[d]o, nell'ambito delle proprie attribuzioni, con le Forze di polizia dello Stato, previa disposizione del sindaco, quando ne venga fatta, per specifiche operazioni, motivata richiesta dalle competenti autorità" (art. 3). A tal fine, il Prefetto conferisce al personale delle Polizia locale, previa comunicazione del Sindaco, la qualità di agente di pubblica sicurezza, dopo aver accertato il possesso dei requisiti previsti dalla legge (art. 5, comma 2). Nell'esercizio delle funzioni di agente di pubblica sicurezza, tale personale, messo a disposizione dal Sindaco, dipende operativamente dalla competente autorità di pubblica sicurezza nel rispetto di eventuali intese fra le dette autorità e il Sindaco (art. 5, comma 4). Conseguentemente, non risultando in atti alcuna indicazione proveniente dalle competenti di autorità di pubblica sicurezza in merito a "specifiche operazioni" e non potendo la Polizia locale del Comune porre di propria iniziativa attività di pubblica sicurezza di carattere generale e preventivo, deve escludersi che l'impiego della telecamera oggetto di segnalazione possa ricondursi all'ambito della pubblica sicurezza (cfr., al riguardo il recente provv. 11 gennaio 2024, n. 5, doc. web n. 9977020, par. 4).

Il Comune ha poi sostenuto che tale telecamera sarebbe stata impiegata nel differente ambito dell'attività di polizia giudiziaria, su impulso del Sindaco, "quale Ufficiale di Polizia Giudiziaria ex art. 57, comma 1 lett. c c.p.p.", sul presupposto della sussistenza di "gravi indizi a carico della segnalante consistiti nel mancato adempimento delle "formalità previste per la rilevazione delle presenze"" (v. memoria difensiva). Nel rilevare che non vi è evidenza in atti che il Comune - in persona del Sindaco (cfr. art. 55, comma 3, c.p.p. e art. 57, comma 1, lett. c), c.p.p.) o tramite agenti della Polizia locale (cfr. art. 55, comma 3, c.p.p. e art. 5, parr. 1, lett. a), e 4 della l. 7 marzo 1986, n. 65) - abbia svolto, nel caso di specie, attività di polizia giudiziaria su impulso, alla dipendenza e sotto la direzione dell'autorità giudiziaria (cfr. artt. 55, comma 2, e 56 c.p.p.), si osserva che, diversamente da quanto prospettato dal titolare del trattamento, risulta invece in atti che il Sindaco ha sporto specifica querela nei confronti della lavoratrice interessata, senza peraltro fare alcun riferimento a prove acquisite mediante dispositivi di videosorveglianza o a un'asserita attività delegata dall'autorità giudiziaria (v. all. 9 alla memoria difensiva; in merito ai presupposti che giustificano le attività di polizia giudiziaria da parte dei Comuni tramite il Corpo di polizia locale, v. provv. 16 novembre 2023, n. 577, doc. web n. 9963453).

Al concreto trattamento posto in essere mediante la telecamera di videosorveglianza in questione trova, invece, applicazione il comma 1 dell'art. 4, della l. 300/1970 come, d'altra parte, comprovato dalla circostanza che l'Ispettorato territoriale del lavoro di Cremona aveva effettuato un'attività ispettiva presso il Comune, a seguito della quale lo stesso aveva disattivato la telecamera in questione e che, successivamente, con "domanda pervenuta in data XX e perfezionata in data XX", aveva chiesto al predetto Ispettorato, l'autorizzazione ai sensi del predetto art. 4, comma 1, della l. 300/1970 a installare "un impianto di controllo a distanza [della] sede, sulla base di esigenze [di] tutela del patrimonio aziendale" (v. provvedimento del predetto Ispettorato n. XX del XX, in atti). Lo stesso titolare del trattamento, nel corso dell'istruttoria, ha altresì invocato esigenze comunque riconducibili al comma 1, dell'art. 4, della l. 300/1970, in particolare, oltre a quelle della tutela del proprio patrimonio anche quelle di tutela della sicurezza dei lavoratori, sul presupposto che nel mese di XX si era verificata un'aggressione ai danni di un'assistente sociale e di un assessore.

Chiarito il contesto di riferimento, occorre ricordare che il Garante, richiamando anche la giurisprudenza della Corte europea dei diritti dell'uomo, nel caso Antovic e Mirkovic v. Montenegro (Application n. 70838/13 del 28 novembre 2017), ha in più occasioni evidenziato che la videosorveglianza nei contesti lavorativi, tanto privati quanto pubblici, 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 Convenzione europea dei diritti dell'uomo.

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 pubblici, da ultimo, provv.16 novembre 2023, n. 578, doc. web n. 9963486, ma anche, provv.ti 11 marzo 2021, n. 90, doc. web n. 9582791 e 5 marzo 2020, n. 53, doc. web n. 9433080, in particolare punto 4.2, nonché i precedenti in essi richiamati; a livello europeo, v. le "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", cit., spec. par. 48, nonché le precedenti indicazioni del Gruppo di Lavoro Articolo 29 nel "Parere 2/2017 sul trattamento dei dati sul posto di lavoro", WP 249, dell'8 giugno 2017; in giurisprudenza, v. Cass. pen., sez. 3, 17 dicembre 2019, n. 50919).

Nel caso di specie, risulta accertato che, nel periodo intercorrente tra il mese di XX e il XX, il Comune ha trattato dati personali relativi ai propri lavoratori, ovvero le immagini acquisite mediante la telecamera di videosorveglianza in questione, in assenza di un accordo con le organizzazioni sindacali o di un'autorizzazione concessa dall'Ispettorato del Lavoro, che risulta essere stato invece ottenuta in data XX e, dunque, fino a tale data non rispettando i presupposti e le garanzie previsti dalla richiamata disciplina di settore in materia di controlli a distanza, in violazione degli artt. 5, par. 1, lett. a), 6 e 88 del Regolamento, nonché 114 del Codice, in riferimento all'art. 4, comma 1, della l. n. 300 del 1970.

Per quanto attiene al connesso profilo della correttezza e trasparenza del trattamento, deve osservarsi che, allorquando siano impiegati sistemi di videosorveglianza, 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 (sportello informazioni, reception, cassa, ecc.) 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 citato "Provvedimento in materia di videosorveglianza" del Garante dell'8 aprile 2010, in particolare par. 3.1; v., da ultimo, le recenti FAQ del Garante in materia di videosorveglianza, cit., n. 4). 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'Unione europea, e del periodo di conservazione. 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, par. 115)). La segnaletica di avvertimento recante l'informativa di primo livello deve contenere un chiaro riferimento al secondo livello d'informazioni, ad esempio, indicando un sito web sul quale è possibile consultare il testo dell'informativa estesa (cfr., con specifico riguardo all'impiego di telecamere di videosorveglianza nei luoghi di lavoro pubblici, provv.ti 16 novembre 2023, n. 578, doc. web n. 9963486 e 11 marzo 2021, n. 90, doc. web n. 9582791; più in generale, con riguardo all'impiego di dispositivi video da parte di Comuni, cfr., da ultimo, provv. 11 gennaio 2024, n. 5, 11 gennaio 2024, e i precedenti in esso richiamati).

Ciò premesso, nel prendere atto di quanto dichiarato dal Comune in sede di memoria difensiva in merito alla circostanza che era stata installata "cartellonistica [...] nelle immediate vicinanze delle videocamere dislocate", si deve rilevare che il Comune ha, tuttavia, omesso di fornire agli

interessati un'ideale informativa estesa, di secondo livello, sul trattamento dei dati personali. Il Comune si è, infatti, limitato a sostenere di aver assolto ai propri obblighi informativi con la pubblicazione del regolamento comunale sulla videosorveglianza, approvato con delibera n. 26 del 29 giugno 2005. Al riguardo, si osserva che tale documento non contiene tutti gli elementi informativi essenziali richiesti dall'art. 13 del Regolamento (ad esempio, la finalità e la base giuridica dei trattamenti effettuati mediante telecamere poste all'interno della sede del Comune, quale luogo di lavoro; i dati di contatto del responsabile della protezione dei dati), essendo stato, peraltro, approvato ben prima della data di efficacia dello stesso. Infatti, lo stesso "disciplina le modalità di raccolta, trattamento e conservazione dei dati personali attivati nel territorio urbano del Comune di Madignano e collegati alla postazione di controllo e di videoregistrazione" (art. 4) e non ha, invece, lo scopo di assolvere agli obblighi informativi nei confronti degli interessati. Lo stesso art. 5 ("Informativa") del medesimo regolamento prevede, d'altra parte, che "gli interessati devono essere informati che stanno per accedere o che si trovano in una zona videosorvegliata, e dell'eventuale registrazione, mediante un modello semplificato di informativa "minima"", mentre "in luoghi diversi dalle aree esterne il modello va integrato con almeno un avviso circostanziato che riporti gli elementi indicati dall'art. 13 del Codice [nel testo al tempo vigente], con particolare riguardo alle finalità e all'eventuale conservazione".

Per quanto attiene più specificamente ai lavoratori in servizio presso il Comune, deve osservarsi che, come già evidenziato dal Garante in precedenti decisioni, atti e documenti che, come nel caso di specie, sono redatti dal datore di lavoro per assolvere ad obblighi diversi rispetto a quelli derivanti dalla disciplina in materia di protezione dei dati, non possono sostituire l'informativa che il titolare deve rendere, prima di iniziare il trattamento, agli interessati in merito alle caratteristiche essenziali dello stesso; ciò allo scopo di consentire all'interessato di esser pienamente consapevole della tipologia di operazioni di trattamento che potranno essere svolte anche attingendo, in un quadro di liceità, ai dati raccolti nel corso dell'attività lavorativa (v., in particolare, provv. 13 maggio 2021, 190, doc. web n. 9669974, che richiama le Sentenze della Corte europea dei diritti dell'uomo del 5 settembre 2017 - Ricorso n. 61496/08 - Causa Barbulescu c. Romania, spec. par. n.133 e 140 e del 9 gennaio 2018- ricorso n. 1874/13 e 8567/13- Causa López Ribalda e altri v. Spagna, spec. par. n. 115; cfr. Gruppo di Lavoro art. 29, "Linee guida sulla trasparenza ai sensi del regolamento 2016/679" dell'11 aprile 2018, par. 17).

D'altra parte, il regolamento comunale sulla videosorveglianza è stato approvato il XX, ossia ben prima dell'adozione del provvedimento autorizzativo dell'Ispettorato territoriale del lavoro di Cremona del XX, non potendo, pertanto, tale regolamento dar conto della specifica base giuridica (cfr. art. 13, par. 1, lett. c), del Regolamento) sui cui, nel caso di specie, poteva fondarsi il trattamento dei dati personali dei lavoratori (art. 6, par. 1, lett. c), e 88 del Regolamento; art. 4, comma 1, della l. 300/1970; art. 114 del Codice).

Alla luce delle considerazioni che precedono, deve concludersi che il Comune non ha fornito agli interessati (ovvero sia lavoratori che utenti o visitatori presso la propria sede) un'ideale informativa sul trattamento dei dati, completa di tutti gli elementi richiesti dal Regolamento, in violazione degli artt. 5, par. 1, lett. a), 12 e 13 del Regolamento.

### **3.3. L'utilizzo dei dati raccolti mediante il sistema di videosorveglianza per fini disciplinari.**

Nel corso dell'istruttoria è stato, inoltre, accertato che, con nota una del XX, il Segretario comunale ha trasmesso all'Ufficio Procedimenti Disciplinari della Provincia di Cremona una segnalazione di fatti aventi rilevanza disciplinare a carico della lavoratrice interessata. In tale nota veniva, in particolare, contestata la scorretta rappresentazione della presenza in servizio, sul presupposto che la dipendente avrebbe omesso di timbrare il cartellino in uscita nei giorni XX e XX. Veniva, altresì, contestata all'interessata l'introduzione di persone estranee all'amministrazione nei locali del Comune in data XX.

Nella predetta nota di trasmissione all'Ufficio competente il Segretario comunale, nel dare conto

che l'amministrazione aveva appreso le condotte poste in essere dalla dipendente, avendo ricevuto segnalazioni da parte di terzi, e che "il Comune è dotato di sistema di videosorveglianza concernente, fra l'altro, l'ingresso alla sede comunale e l'atrio di accesso agli uffici" (v. premessa di cui alla lett. b)), riportava una specifica dichiarazione del Sindaco, ovvero che lo stesso aveva "personalmente [...] visionato le telecamere comunali per verificare la veridicità delle segnalazioni riscontrandone puntualmente la fondatezza: appena dopo aver timbrato la dipendente è uscita dal comune per farvi ritorno poco dopo" (cfr. all. 1 alla predetta nota del XX), con ciò confermando che le contestazioni disciplinari in questione sono state avanzate nei confronti dell'interessata anche sulla base dell'effettivo esame delle immagini di videosorveglianza.

Tale circostanza trova, altresì, riscontro dalla documentazione in atti relativa al procedimento disciplinare, in quanto, nel provvedimento dell'Ufficio per i Procedimenti Disciplinari della Provincia di Cremona prot. n. XX del XX (con il quale veniva irrogata la sanzione disciplinare all'interessata in relazione alle predette condotte) nel replicare a quanto prospettato dal legale dell'interessata circa la "la violazione dell'art. 4 della l. 300/1970", si precisa che "in ordine alla presunta violazione dell'art. 4 dello Statuto dei lavoratori [...] [sono] fuori dall'ambito di applicazione della norma il controllo per la tutela patrimoniale così come i controlli diretti ad accertare condotte illecite del lavoratore, tanto più ex post, ossia dopo l'attuazione del comportamento in addebito, così da prescindere dalla mera sorveglianza sull'esecuzione della prestazione lavorativa (in tal senso Cass. 3255/2021)".

Si deve, invece, evidenziare nuovamente 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 (art. 5, par. 1, lett. a), 6, 88, par. 1, del Regolamento, nonché 114 del Codice, in riferimento all'art. 4 della l. n. 300/1970).

Come pure di recente ribadito dal Garante, a seguito delle modifiche apportate all'art. 4 della l. n. 300/1970 dal d.lgs. 14 settembre 2015, n. 151, anche le esigenze di tutela del patrimonio datoriale sono state espressamente incluse 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 sprovvisto di idonea base giuridica e quindi illecito (v. provv. 1° dicembre 2022, n. 409, doc. web n. 9833530). Conseguentemente, le forme di controllo sull'attività dei lavoratori, poste 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.

Si consideri, altresì, che la predetta disciplina di settore consente 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. 300/1970). Tali successive ed eventuali operazioni di trattamento presuppongono il rispetto del quadro normativo di riferimento sia in materia di controlli a distanza dei lavoratori (ai sensi dei commi 1 e 2) che in materia di protezione dei dati. Ciò anche con riguardo alla necessità di fornire agli interessati ogni necessaria informazione per assicurare ai dipendenti piena consapevolezza degli ulteriori trattamenti che il datore di lavoro si riserva di effettuare (sul punto, v. provv. 1° dicembre 2022, n. 409, cit.; 28 ottobre 2021, n. 384, doc. web n. 9722661; 13 maggio 2021, n.

190, doc. web n. 9669974; v. già provv. 24 maggio 2017, n. 247, doc. web n. 6495708, spec. punto 5.3 e lett. e) dispositivo).

Nel caso di specie, impregiudicate le valutazioni espresse al precedente par. 3.2 in merito all'impiego del predetto sistema di videosorveglianza in assenza delle garanzie di cui all'art. 4, comma 1, della l. 300/1970, risulta che il provvedimento disciplinare in questione è stato adottato il XX, ovvero in data antecedente a quella in cui è stata ottenuta l'autorizzazione dell'Ispettorato territoriale del lavoro all'installazione di detta telecamera, senza aver fornito ai dipendenti un'adeguata informazione in merito alle modalità con cui lo stesso si riservava di utilizzare i predetti dati nell'ambito del rapporto di lavoro ai sensi del comma 3 del predetto art. 4.

Da ultimo, anche alla luce di quanto prospettato dal Comune, si ricorda che in tale quadro il Garante ha chiarito che "la c.d. teoria sui controlli difensivi, di pura creazione giurisprudenziale, è oggetto di applicazioni non univoche" (cfr., sul punto, provv.ti 1° dicembre 2022, n. 409, cit., e 15 aprile 2021, n. 137, doc. web n. 9670738) e si fonda su circostanze di fatto che in ogni caso non ricorrono nel caso di specie (avendo il Comune installato la telecamera di videosorveglianza anteriormente ai fatti poi contestati alla dipendente e in maniera tale da riprendere la totalità dei lavoratori e dei visitatori transitanti nell'atrio dell'edificio); infatti, come già evidenziato, le esigenze di tutela del patrimonio datoriale sono state espressamente incluse tra le lecite finalità perseguibili mediante sistemi di videosorveglianza, subordinandone l'installazione e l'utilizzazione all'accordo sindacale o, in alternativa, all'autorizzazione pubblica (art. 4, comma 1, l. 300/1970).

Per tali ragioni, si deve concludere che l'utilizzo, da parte del Comune, di dati raccolti mediante il predetto sistema di videosorveglianza, nell'ambito del procedimento disciplinare avviato nei confronti della segnalante, sia avvenuto in violazione tanto della disciplina di settore in materia di controlli a distanza quanto di quella 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.

#### **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 dal Comune, per aver trattato dati personali mediante un dispositivo video, anche a fini disciplinari nei confronti di una dipendente, e in assenza di trasparenza nei confronti degli interessati, in violazione degli artt. 5, par. 1, lett. a) e b), 6, 12, 13 e 88 del Regolamento, nonché 114 del Codice (in riferimento all'art. 4, commi 1 e 3, della l. n. 300 del 1970).

Tenuto conto che la violazione delle predette disposizioni ha avuto luogo in conseguenza di un'unica condotta, 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, tutte le violazioni sono soggette alla sanzione prevista dall'art. 83, par. 5, del Regolamento, 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).**

L'art. 58, par. 2, del Regolamento attribuisce al Garante il potere di "ingiungere al titolare del

trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine” (lett. d).

Sulla base di quanto emerso all’esito dell’istruttoria in relazione agli obblighi in materia di trasparenza, si rende necessario, ai sensi dell’art. 58, par. 2, lett. d), del Regolamento, ingiungere al Comune di fornire a tutti gli interessati (ovvero sia i lavoratori sia i visitatori presso la sede del Comune), ai sensi degli artt. 5, par. 1, lett. a), 12 e 13 del Regolamento, un’idonea informativa sul trattamento dei dati personali, raccolti e trattati mediante la telecamera di videosorveglianza in questione, contenente tutti gli elementi informativi essenziali di cui all’art. 13 del Regolamento.

Ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, il Comune dovrà, inoltre, provvedere a comunicare all’ 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 ordinato ai sensi del citato art. 58, par. 2, lett. d), nonché le eventuali misure poste in essere per assicurare la conformità del trattamento alla normativa in materia di protezione dei dati personali.

#### **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.

In relazione ai predetti elementi, è stata considerata la specifica natura del trattamento, avviato in modo non conforme alla disciplina di settore in materia di impiego di strumenti che possono comportare un monitoraggio dell’attività lavorativa e alle indicazioni fornite nel tempo dal Garante, per i profili di competenza (cfr. art. 83, par. 1, lett. a), del Regolamento).

Si è, inoltre, tenuta in considerazione la circostanza che il Comune, nonostante l’avvio dell’istruttoria da parte dell’Autorità, non ha comprovato di aver provveduto a fornire agli interessati (cittadini, visitatori e dipendenti) una specifica informativa sul trattamento dei dati personali mediante la telecamera di videosorveglianza in questione (cfr. art. 83, par. 1, lett. a), del Regolamento).

Per le predette ragioni, 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, “Guidelines 04/2022 on the calculation of administrative fines under the GDPR” del 23 maggio 2023, punto 60).

Ciò premesso, si deve considerare, in senso favorevole al titolare, che quest'ultimo è un Comune di modeste dimensioni (circa 2.700 abitanti) e che, ai fini dell'83, par. 2, lett. e), del Regolamento, non risultano precedenti violazioni pertinenti commesse dal titolare del trattamento o precedenti provvedimenti di cui all'art. 58 del Regolamento.

Infine, ai fini dell'art. 83, par. 2, lett. k), del Regolamento, si ritiene debba considerarsi che la violazione ha riguardato una specifica articolazione interna del titolare del trattamento e non la complessiva organizzazione dello stesso.

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 3.000 (tremila) per la violazione degli artt. 5, par. 1, lett. a) e b), 6, 12, 13 e 88 del Regolamento, nonché 114 del Codice (in riferimento all'art. 4, commi 1 e 3, della l. n. 300/1970), quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

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

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

### **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 Madignano per violazione degli artt. 5, par. 1, lett. a) e b), 6, 12, 13 e 88 del Regolamento, nonché 114 del Codice (in riferimento all'art. 4, commi 1 e 3, della l. n. 300/1970), nei termini di cui in motivazione;

### **ORDINA**

al Comune di Madignano, in persona del legale rappresentante pro-tempore, con sede legale in Via Libertà, 22 - 26020 Madignano (CR), C.F. 00302860192, di pagare la somma di euro 3.000 (tremila) 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 3.000 (tremila) 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;

- ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, di fornire a tutti gli interessati (ovvero sia i lavoratori sia i visitatori presso la sede del Comune), ai sensi degli artt. 5, par. 1, lett. a), 12 e 13 del Regolamento, un'idonea informativa sul trattamento dei dati personali, contenente tutti gli elementi informativi essenziali di cui all'art. 13 del Regolamento;

- 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 disposto nel presente punto può comportare l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento;

### **DISPONE**

- la pubblicazione del presente provvedimento sul sito web del Garante ai sensi dell'art. 166, comma 7, del Codice (v. art. 16 del Regolamento del Garante n. 1/2019);

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

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.

*Messina, 11 aprile 2024*

IL PRESIDENTE  
Stanzione

IL RELATORE  
Scorza

IL SEGRETARIO GENERALE  
Mattei