



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

## **Provvedimento del 19 dicembre 2024 [10107263]**

[doc. web n. 10107263]

**Provvedimento del 19 dicembre 2024**

Registro dei provvedimenti  
n. 805 del 19 dicembre 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 dott. Claudio Filippi, vice 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 la prof.ssa Ginevra Cerrina Feroni;

### **PREMESSO**

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

L’Autorità ha appreso da un articolo di stampa che il Comune di Levanto (di seguito, il “Comune”) ha installato sul proprio territorio talune telecamere dotate di funzionalità di lettura automatizzata delle targhe dei veicoli in transito, allo scopo di studiare i flussi turistici, attraverso l’individuazione della provincia italiana o dello Stato di immatricolazione.

In un comunicato stampa pubblicato sul sito web istituzionale del Comune veniva, altresì, affermato che lo stesso impiegherebbe “121 telecamere di ultima generazione”, dotate di funzionalità di “controllo e ricerca degli eventi”, e di “6 telecamere di lettura targhe agli ingressi cittadini che verificano costantemente lo stato di revisione assicurativo dei veicoli e dei motocicli” e consentono di “analizzare sia il flusso di provenienza dei veicoli, suddividendoli per nazione per quanto riguarda il traffico straniero e in province per il traffico nazionale, che il flusso dei veicoli più inquinanti attraverso l’analisi dell’omologazione Euro di veicoli e motocicli”, nonché “di fare ricerche sul colore, la dimensione e la marca dei veicoli: vale a dire le caratteristiche che immediatamente emergono dalle prime testimonianze di chi ha assistito al transito di auto in fuga da incidenti o da rapine e furti”.

Il medesimo comunicato stampa riportava, inoltre, i principali dati relativi alla provincia di provenienza di circa 512.000 veicoli transitati nel territorio comunale tra il XX e il XX.

## **2. L’attività istruttoria.**

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

“il sistema di videosorveglianza [del Comune] consta di 118 telecamere di contesto di ultima generazione [...] delle quali 110 [...] già attive e 8 in fase di implementazione - installate per soddisfare tipiche finalità istituzionali dell’Ente, come la sicurezza e il controllo del territorio comunale (in particolare, indagini/accertamenti su atti predatori e vandalismi)”;

“esistono, poi, 5 telecamere di lettura targhe presso le vie di accesso al territorio comunale che rilevano il flusso veicolare, di cui solo una presenta caratteristiche tecniche che consentono l’utilizzo delle “funzionalità avanzate” di ricerca di colore, modello, tipologia e marca dei veicoli (mediante [un] software [fornito da un’azienda - di seguito, il “Software”])”;

“a seguito dell’attivazione delle [predette cinque] telecamere [...] è possibile effettuare rilievi statistici mediante il Software con un processo automatizzato di separazione dei dati che estrae dati anonimi e statistici [...] [, che risulta] estrane[o] al campo di applicazione della disciplina sul trattamento dei dati personali [...], per le attività di gestione del traffico e dei flussi turistici”;

“il dispositivo video che consente di utilizzare le “funzionalità avanzate” [...] è stato installato il XX mentre l’attivazione è stata effettuata il XX”;

“in merito alla finalità di trattamento perseguita e alla normativa di settore [il Comune] rimand[a] [alla] Nota del Ministero dell’Interno [, ovvero alla circolare XX del XX,] specificando che le contestazioni vengono effettuate in tempo reale” e, pertanto, “in merito all’omologazione dei dispositivi di videosorveglianza, la stessa non è necessaria in quanto le contestazioni vengono effettuate in tempo reale (con la verifica della documentazione da parte della Polizia Locale) e non in modalità differita”, tramite “le banche dati della Motorizzazione civile [...] e specifica interrogazione ai sensi del DPR 634/1994”.

In allegato alla predetta nota, il Comune ha prodotto in atti una relazione tecnica, dalla quale emerge, in particolare, che:

le cinque telecamere in questione “acquisiscono i numeri di targa di tutti i veicoli in transito e le inviano al Software [...] che provvede all’archiviazione dei dati delle targhe per un tempo di 180 giorni e per le immagini per un tempo di 7 giorni nel formato criptato [...] con password. [...] Il software si collega alle banche dati Ministeriali (Motorizzazione)”;

“il [Software] è provvisto di moduli e algoritmi di analisi video che determinano la Marca ed il

Modello, Tipo, Colore e Classificazione ambientale dei veicoli utili per la ricerca particolare nei transiti archiviati e per tutte le esigenze degli operatori di Polizia Locale e Forze dell'Ordine. Il Software permette una elaborazione specifica del dato in modo totalmente anonimo per fini statistici in particolare la classificazione dei veicoli per Provincia di appartenenza, per Nazione di provenienza. L'elaborato estratto (grafico numerico o in percentuale) per statistica non può in nessun modo ricondurre ad una specificata targa archiviata”;

“ulteriore funzione statistica “avanzata” è la classificazione EURO dei veicoli che permette di generare un grafico con il numero dei veicoli transitati classificandoli nella tabella da EURO 0 ad EURO 6. Questi dati in totale forma anonima non sono [...] riconducibili alle specifiche targhe transitate sul territorio”;

“sul territorio del Comune [...] sono installate ulteriori 118 telecamere di videosorveglianza di cui 110 attive e 8 in fase di attivazione [...]. Le telecamere sono di tipologia fissa [...]. Per facilitare la ricerca da parte della Polizia Locale di particolari eventi su alcune telecamere è attivata la rilevazione del movimento (motion detection). La rilevazione del movimento è totalmente anonima e non viene effettuata per l'identificazione dei veicoli e delle persone”.

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

“i quattro dispositivi video dotati di funzionalità di lettura targhe (ancorché senza funzionalità avanzate) sono stati installati e attivati dal Comune di Levanto secondo le seguenti tempistiche:

a) [...] tre dispositivi [...] in data XX e attivati in data XX [...];

b) [un] dispositivo [...] è stato installato in data XX2 e attivato a XX [...];”;

“non è disponibile il numero complessivo di targhe rilevate mediante i cinque dispositivi video in questione a partire dalla data di attivazione”;

“l'informativa completa sul trattamento dei dati personali è stata messa a disposizione degli interessati mediante pubblicazione sul sito web istituzionale a partire dal giorno XX”;

“la redazione della valutazione d'impatto è iniziata il XX e perfezionata [...] in data XX [...]”.

Da ultimo, in riscontro a un'ulteriore richiesta d'informazioni (v. nota prot. n. XX dell'XX), il Comune, con nota del XX (prot. n. XX), ha dichiarato, in particolare, che:

“il Comune [...], nella gestione del sistema di videosorveglianza [...] [osserva] il termine massimo di durata della conservazione dei dati [...] limitato ai 7 giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di ripresa e di 180 giorni per quanto attiene ai sistemi di tracciamento targhe e transiti, fatte salve speciali esigenze di ulteriore conservazione”;

in merito alla pubblicazione dell'informativa di secondo livello sul sito web istituzionale del Comune, “la prima “Generazione della pagina WEB” è avvenuta in data XX in ragione della necessità di fornire ai cittadini e a tutti gli interessati adeguata informazione sulla presenza, sul territorio comunale, di un sistema di videosorveglianza, a cui sono, poi, seguiti periodici aggiornamenti”;

“[...] nel XX, il sito del Comune è stato interamente sostituito da un nuovo sito ed è possibile, allo stato attuale, recuperare solo parte dei contenuti presenti a suo tempo, essendo

transitati sul nuovo sito solo i dati necessari all'adempimento degli oneri di Legge e al perseguimento delle finalità istituzionali dell'Ente”;

“le ricerche effettuate hanno consentito di ricostruire la data di creazione della pagina dedicata alla pubblicazione dell'informativa e le date dei successivi aggiornamenti [...] gli aggiornamenti della pagina sono certificati dai relativi log alle seguenti date: XX, XX, XX, XX e XX”;

in merito alla valutazione d'impatto sulla protezione dei dati, “la consegna del documento [è] avvenuta brevi manu, essendo stata commissionata a professionista che all'epoca, svolgeva anche altri servizi per l'Amministrazione ed era, quindi, presente fisicamente nella sede comunale per sovrintendere alle attività di implementazione del sistema di videosorveglianza”.

Con la predetta nota, il Comune ha, altresì, prodotto in atti copia dei patti per l'attuazione della sicurezza urbana stipulati tra il Comune e la Prefettura territorialmente competente negli anni XX e XX.

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 trattato i dati personali relativi alle targhe dei veicoli in transito in maniera non conforme al principio di liceità, correttezza e trasparenza e in assenza di una idonea base giuridica, in violazione degli artt. 5, par. 1, lett. a), e 6 del Regolamento, nonché 2-ter del Codice;

per aver posto in essere un trattamento di dati personali mediante dispositivi video, fornendo agli interessati un'inidonea informativa di primo livello, omettendo di fornire agli stessi un'informativa di secondo livello fino al XX, nonché, dopo tale data, fornendo agli stessi un'inidonea informativa di secondo livello, in violazione degli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento;

per aver omesso di redigere una valutazione d'impatto sulla protezione dei dati prima d'iniziare il trattamento, in violazione dell'art. 35 del Regolamento.

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

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

“i dispositivi video dotati di funzionalità di lettura targhe sono, effettivamente, in funzione su base continuativa”, ma le verifiche di carattere amministrativo sono state effettuate “solo quando [gli agenti della Polizia locale] si trovano sul territorio comunale per effettuare le contestazioni in tempo reale”;

le informazioni sulla provincia di immatricolazione dei veicoli “non sono ricavate mediante interrogazione al Portale dell'Automobilista ma sono desumibili dalle targhe stesse, che riportano lettere e numeri dai quali è possibile individuare i dati della sola provincia relativi alla prima immatricolazione”;

“i dati conservati nel server sono stati utilizzati per il contrasto di fenomeni criminosi a seguito di specifiche richieste dell'Autorità Giudiziaria, delle Forze di Polizia o dei

Carabinieri”;

“il Comune [...], a prescindere dalla pubblicazione di contenuti sul proprio sito, ha sempre reso disponibile l’Informativa di secondo livello presso la sede comunale, come indicato in tutti cartelli esposti”;

“la temporanea indisponibilità di alcune sezioni del sito è stata dovuta a problemi tecnici legati al passaggio dal vecchio al nuovo sito”;

“il Comune [...] ha inserito nell’informativa di primo livello un indirizzo di posta elettronica certificata riferibile all’Amministrazione, ritenendo utile far confluire tutte le richieste formulate dagli interessati al Protocollo del Comune stesso”;

“nell’Informativa di secondo livello era, comunque, presente anche il recapito diretto del RPD/DPO”;

“[il testo] dell’Informativa di secondo livello [nella versione del] XX [è] stat[o] caricato, successivamente, dall’Ufficio Informatico del Comune anche sul sito”;

“in merito alla mancanza di data certa della DPIA [...], il Comune] per un mero errore di valutazione, non ha ritenuto necessario adottare la DPIA mediante apposito atto formale, incorrendo nell’oggettiva impossibilità di dimostrare al Garante la data certa”;

a seguito della notifica della contestazione di violazione amministrativa, “il Comune [...] ha ritenuto doveroso disattivare tutto il sistema di videosorveglianza”.

In occasione dell’audizione, richiesta ai sensi dell’art. 166, comma 6, del Codice e tenutasi in data XX4 (v. verbale prot. n. XX della medesima data), il Comune ha dichiarato, in particolare, che:

“il Comune ha ottenuto degli specifici finanziamenti pubblici ai fini dell’installazione e dell’utilizzo dei sistemi di videosorveglianza in questione, avendo agito, pertanto, in buona fede, confidando operato in linea con le aspettative dei soggetti preposti al controllo dell’ordine pubblico, anche tenuto conto delle specificità del territorio e dell’esigenza molto sentita di assicurare un efficace controllo dello stesso”;

“il Comune ha preferito sospendere l’utilizzo dell’intero sistema di videosorveglianza, in un’ottica di estrema collaborazione con l’Autorità e al fine esclusivo di assicurare il massimo rispetto della normativa in materia di protezione dei dati”;

“per quanto concerne i profili che attengono alla trasparenza, si fa presente che nel passaggio dal precedente sito web istituzionale dell’Ente all’attuale sito si è verificato un disallineamento, che, per un certo arco temporale, non ha consentito di mettere online la versione aggiornata dell’informativa e di permette all’Ente di ricostruire con puntualità le date di pubblicazione delle varie versioni dell’informativa succedutesi nel tempo”;

“i dispositivi video in questione sono stati messi in funzione durante il periodo dell’emergenza epidemiologica da SARS-CoV-2, che, come noto, ha avuto significative ripercussioni sull’attività amministrativa dei soggetti pubblici. In tale delicata fase, il Comune ha dovuto assumere decisioni complesse e in tempi rapidi, anche al fine di poter rispettare i termini previsti dai procedimenti finalizzati alla concessione dei finanziamenti pubblici per la videosorveglianza. Si precisa che il Comune [...] è, peraltro, un piccolo Ente, con una popolazione di circa 5.131 abitanti residenti e con una presenza di circa 30.000 persone nel periodo estivo”;

“la valutazione d’impatto è stata redatta nel corso dello sviluppo e implementazione del

progetto, ancorché l'Ente non sia in grado di provare la data certa del documento, non avendo assunto la versione finale dello stesso al protocollo informatico”;

quanto all'impiego del Software per acquisire il dato sulla provincia/Stato di immatricolazione dei veicoli in transito, “tale funzionalità è stata offerta dal fornitore all'Ente, [e il Comune] in buona fede ha ritenuto di poterne usufruire, nella convinzione che non vi fossero profili di protezione dei dati da tenere in considerazione, sul presupposto che l'Ente [avrebbe] avuto accesso soltanto a dati statistici e aggregati, senza alcuna possibilità di identificare gli interessati”;

“ancorché i dati relativi ai numeri di targa siano stati conservati per 180 giorni, gli stessi sono stati utilizzati dall'Ente esclusivamente nei casi in cui le Forze dell'Ordine hanno chiesto di ottenere informazioni sui transiti nell'ambito di indagini di polizia giudiziaria. Nessun altro trattamento è stato posto in essere utilizzando tali dati e l'accesso agli stessi era consentito esclusivamente al Comandante e a due agenti designati quali agenti di pubblica sicurezza, in ogni caso con sistemi idonei a garantire l'accesso solo ai soggetti autorizzati”.

Successivamente, a scioglimento di talune riserve formulate in sede di audizione, il Comune, con nota del XX (prot. n. XX), ha dichiarato, in particolare, che:

“l'Amministrazione è riuscita a ricostruire puntualmente le date di pubblicazione della documentazione utile per informare adeguatamente gli utenti sul sistema di videosorveglianza. In particolare, si evidenzia la presenza nel precedente sito (così come in quello più recente, direttamente consultabile alla pagina <https://comune.levanto.sp.it/privacy-policy/>) della seguente documentazione, tracciata dai log degli aggiornamenti della pagina privacy relativa alla videosorveglianza sul sito del comune e allegati alla presente risposta: a) dati di contatto del RPD (DPO) del comune di Levanto; b) i diritti dell'interessato; c) regolamento per la disciplina della videosorveglianza; informativa di secondo livello GDPR; e) informativa sistema di videosorveglianza del territorio comunale”;

“le ricerche informatiche effettuate a seguito dell'audizione, pur non consentendo il recupero dei contenuti rimossi (e/o sostituiti da nuove versioni), attestano la data di creazione della pagina dedicata alla prima pubblicazione dell'informativa e le date di successivi caricamenti/modifiche”;

“la nazionalità di immatricolazione del veicolo si ricava grazie alla “lettura “sintattica” della stringa alfanumerica che compone la targa del veicolo”. Viceversa, la provincia di immatricolazione viene attribuita “per indiretto confronto con un data base di pubblico accesso (di cui al sito a carattere associativo: “Associazione Targhisti Italiani”) alimentato dagli utenti su base volontaria e anonimizzata.”. Inoltre, la Società interpellata dichiara che: “L'anzidetto database, infatti: i) contiene esclusivamente vari elenchi di intervalli alfa numerici di parti di targhe di autoveicoli attribuiti alle varie province italiane che non consentono, nemmeno indirettamente, alcuna identificazione di persone fisiche a cui gli autoveicoli in questione potrebbero appartenere; ii) risulta periodicamente aggiornato in forma aggregata e statistica su base volontaria e, su tali basi, costituisce la fonte che permette la determinazione “in locale” della “possibile provincia di immatricolazione degli autoveicoli le cui targhe possono essere rese oggetto di funzionalità del Software”.

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

#### **3.1 La liceità del trattamento.**

All'esito dell'attività istruttoria, è emerso che il Comune si è dotato di:

un sistema di videosorveglianza, composto da n. 118 telecamere (di cui otto in fase di

attivazione), per il perseguimento delle “tipiche finalità istituzionali dell’Ente, come la sicurezza e il controllo del territorio comunale (in particolare, indagini/accertamenti su atti predatori e vandalismi)”. Su alcune di tali telecamere è attivata una funzionalità di rilevazione del movimento, che non è volta a identificare veicoli o persone, consentendo alla Polizia locale di ricercare particolari eventi ripresi;

n. 5 telecamere non omologate che consentono la lettura automatizzata delle targhe dei veicoli in transito. Tali telecamere sono in grado di determinare la provincia e la nazione di immatricolazione di tali veicoli; una di esse, attivata in data XX, può, inoltre, rilevare la tipologia di veicolo, la marca, il modello e il colore di tali veicoli, nonché la loro classificazione EURO (v. relazione tecnica, cit.). Dei quattro dispositivi non dotati di funzionalità avanzate, tre sono stati attivati in data XX e uno nel mese di XX. I dispositivi in questione consentono di effettuare elaborazioni statistiche in merito allo Stato o alla provincia dei veicoli in intransito, nonché di supportare la Polizia locale nelle attività di verificare dell’assolvimento degli obblighi in materia di revisione e assicurazione obbligatoria, previsti dal Codice della Strada (d.lgs. 30 aprile 1992, n. 285). Il sistema è configurato per effettuare l’“archiviazione dei dati delle targhe per un tempo di 180 giorni e per le immagini per un tempo di 7 giorni” (v. relazione tecnica, cit.).

Ciò premesso, deve osservarsi che i soggetti pubblici possono, di regola, trattare dati personali mediante dispositivi video se il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento o per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri di cui è investito lo stesso (v. art. 5, par. 1, lett. a), 6, parr. 1, lett. c) ed e), 2 e 3, del Regolamento, nonché art. 2-ter del Codice; cfr. le “Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video”, adottate dal Comitato europeo per la protezione dei dati il 29 gennaio 2020, par. 41; v. anche le FAQ del Garante in materia di videosorveglianza, del 3 dicembre 2020, doc. web n. 9496574).

Il titolare del trattamento è tenuto, in ogni caso, a rispettare i principi in materia di protezione dei dati, fra i quali quelli di “liceità, correttezza e trasparenza” e “minimizzazione dei dati”, in base ai quali i dati personali devono essere “trattati in modo lecito, corretto e trasparente nei confronti dell’interessato”, nonché “adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati” (art. 5, par. 1, lett. a) e c), del Regolamento).

Nel caso di specie, il Comune ha impiegato cinque telecamere che consentono la lettura automatizzata delle targhe dei veicoli in transito, di cui una dotata di una funzionalità avanzata che consente l’acquisizione di dati ulteriori (tipologia di veicolo, marca, modello, colore classificazione EURO), al fine di verificare l’assolvimento degli obblighi in materia di revisione e assicurazione obbligatoria, previsti dal Codice della Strada.

Come dichiarato dall’Ente, le contestazioni delle violazioni sono state effettuate in conformità alle modalità previste dalla circolare del Ministero dell’Interno n. XX del XX, che ammette l’utilizzo di dispositivi video non omologati come mero strumento di supporto agli agenti della Polizia locale, fisicamente presenti nelle aree interessate dai controlli, ai fini dell’individuazione dei veicoli da fermare e della contestazione immediata delle violazioni eventualmente accertate dagli agenti, salvo che ricorra una situazione di fatto che renda impossibile l’arresto del veicolo e la contestazione immediata, con motivazioni da indicare dettagliatamente nel verbale.

Tuttavia, come è emerso dall’istruttoria, i dispositivi video in questione raccoglievano i numeri di targa di tutti i veicoli in transito su base continuativa, ovvero indipendentemente dall’accertamento di una violazione del Codice della Strada, e il Comune conservava gli stessi per 180 giorni, al dichiarato fine di poter corrispondere a specifiche richieste dell’autorità giudiziaria o delle Forze dell’Ordine, nell’ambito delle attività d’indagine di loro competenza, seppur, come dichiarato dal Comune in sede di audizione, senza trattare gli stessi per altre finalità di natura amministrativa.

Al riguardo, deve osservarsi che la disciplina di settore consente ai Comuni l'impiego di telecamere di videosorveglianza ai soli fini di prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria, previa stipula di un accordo per l'attuazione della sicurezza urbana con la Prefettura territorialmente competente (v. artt. 4 e 5, co. 2, lett. a), del d.l. 20 febbraio 2017, n. 14; v. anche art. 6, co. 7 e 8, del d.l. 23 febbraio 2009, n. 11; cfr. provv.ti 11 gennaio 2024, n. 5, doc. web n. 9977020 e 20 ottobre 2022, n. 341, doc. web n. 9831369). In disparte da ogni considerazione in merito all'idoneità di tale base giuridica a giustificare l'impiego da parte di Comuni di dispositivi video, non omologati, dotati di funzionalità di lettura automatizzata delle targhe dei veicolo in transito, per la tutela della sicurezza urbana, peraltro per un arco temporale, pari a 180 giorni, significativamente più lungo rispetto al termine di sette giorni previsto per la conservazione dei filmati di videosorveglianza (v. art. 6, comma 8, del d.l. 23 febbraio 2009, n. 11), occorre, in ogni caso, rilevare che, nel caso di specie, i patti per l'attuazione della sicurezza urbana stipulati dal Comune con la Prefettura della Spezia il XX e il XX, depositati in atti, non prevedono l'impiego di dispositivi dotati di tale funzionalità per il perseguimento della finalità di prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria. Pertanto, nel caso di specie, i trattamenti di dati personali in questione non possono essere ricondotti alla disciplina in materia di videosorveglianza per la tutela della sicurezza urbana di cui agli artt. 4 e 5, co. 2, lett. a), del d.l. 20 febbraio 2017, n. 14.

Alla luce delle considerazioni che precedono, deve concludersi che, impiegando su base continuativa i cinque dispositivi video in questione per la lettura dei numeri di targa dei veicoli in transito e per la loro successiva conservazione per 180 giorni, in assenza di presupposti di liceità, il Comune ha posto in essere un trattamento di dati personali in maniera non conforme al principio di liceità, correttezza e trasparenza, in violazione degli artt. 5, par. 1, let. a), e 6 del Regolamento nonché 2-ter del Codice.

Quanto, invece, alle altre funzionalità avanzate di cui alcuni dispositivi video erano dotati (rilevazione del movimento), dall'istruttoria non è emerso né che tali funzionalità implicassero l'assunzione di decisioni nei confronti degli interessati basate unicamente sul trattamento automatizzato (cfr. art. 22 del Regolamento) né che il Comune si sia, in ogni caso, effettivamente avvalso delle stesse in casi concreti.

Inoltre, in merito ai trattamenti posti in essere per finalità statistiche (provincia/Stato di immatricolazione del veicolo; tipologia di veicolo, la marca, il modello e il colore di tali veicoli, nonché classificazione EURO), mediante un Software fornito da un'azienda terza, risulta assorbente la circostanza che non sussistesse a monte un'idonea base giuridica che consentisse la raccolta e la conservazione dei numeri di targa di tutti i veicoli in transito, prendendosi comunque atto di quanto dichiarato dal Comune, successivamente all'audizione con l'Autorità, della circostanza che la nazionalità di immatricolazione dei veicoli in transito sarebbe stata meramente dedotta dal formato della targa, mentre la provincia di immatricolazione sarebbe stata determinata per "indiretto confronto" con una banca dati di pubblico accesso, tenuta da un sito web di carattere associativo e alimentata dagli utenti su base volontaria, che conterrebbe "elenchi di intervalli alfa numerici di parti di targhe di autoveicoli attribuiti alle varie province italiane che non consentono, nemmeno indirettamente, alcuna identificazione di persone fisiche".

### **3.2. La trasparenza nei confronti degli interessati.**

Allorquando siano impiegati dispositivi video, il titolare del trattamento, oltre a rendere l'informativa di primo livello mediante apposizione di segnaletica di avvertimento in prossimità della zona sottoposta a videosorveglianza, deve fornire agli interessati anche delle "informazioni di secondo livello", che devono "contenere tutti gli elementi obbligatori a norma dell'articolo 13 del [Regolamento]" ed "essere facilmente accessibili per l'interessato, ad esempio attraverso un pagina informativa completa messa a disposizione in uno snodo centrale [...] o affissa in un luogo di facile accesso" ("Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", cit., in particolare par. 7; ma si veda già il "Provvedimento in materia di videosorveglianza"



del Garante dell'8 aprile 2010, doc. web n. 1712680, in particolare par. 3.1; da ultimo, v. la FAQ del Garante in materia di videosorveglianza, cit., n. 4; cfr., altresì, provv.ti 11 gennaio 2024, n. 5, doc. web n. 9977020; 20 ottobre 2022, n. 341, doc. web n. 9831369; 28 aprile 2022, n. 162, doc. web n. 9777974, 7 aprile 2022, n. 119, doc. web n. 9773950, 16 settembre 2021, n. 327, doc. web n. 9705650 e 11 marzo 2021, n. 90, doc. web n. 9582791).

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 del Comitato, cit., par. 114). Inoltre, la segnaletica deve contenere anche quelle informazioni che potrebbero risultare inaspettate per l'interessato. Potrebbe trattarsi, ad esempio, della trasmissione di dati a terzi, in particolare se ubicati al di fuori dell'UE, e del periodo di conservazione dei dati. Se tali informazioni non sono indicate, l'interessato dovrebbe poter confidare nel fatto che vi sia solo una sorveglianza in tempo reale, senza alcuna registrazione di dati o trasmissione a soggetti terzi (Linee guida del Comitato, cit., par. 115). La segnaletica di avvertimento di primo livello deve contenere un chiaro riferimento al secondo livello di informazioni, ad esempio indicando un sito web sul quale è possibile consultare il testo dell'informativa estesa.

Nel caso di specie, il Comune ha prodotto in atti copia di un cartello, contenente l'informativa sul trattamento dei dati personali di primo livello (v. all. 7 alla nota prot. n.XX del XX). Tale informativa non risulta, tuttavia, conforme ai requisiti previsti dal Regolamento (v. artt. 12, par. 1 e 13), in quanto:

le finalità di trattamento sono indicate in modo del tutto generico (“sicurezza e tutela delle persone fisiche e del patrimonio del Comune di Levanto”), non vi è alcuna menzione delle finalità amministrative connesse alla verifica dell'assolvimento degli obblighi in materia di revisione e assicurazione previsti dal Codice della Strada, né è indicata la base giuridica del trattamento (v. art. 13, par. 1, lett. c), del Regolamento);

è indicato il periodo di conservazione delle immagini (“7 giorni”) ma non vi è alcuna indicazione in relazione al tempo di conservazione dei dati relativi ai numeri di targa, pari a 180 giorni (v. art. 13, par. 2, lett. a), del Regolamento);

i dati di contatto del Responsabile della protezione dei dati (RPD), indicati nel cartello, coincidono con l'indirizzo PEC istituzionale del Comune (comune.levanto.sp@legalmail.it), gli interessati non essendo stati, pertanto, messi in condizione di contattare direttamente il RPD (v. art. 13, par. 1, lett. b), del Regolamento);

è indicato un sito web (“[http://comune.levanto.sp.it/protezione\\_dati\\_personali\\_privacy.html](http://comune.levanto.sp.it/protezione_dati_personali_privacy.html)”), sul quale gli interessati possono rinvenire il testo dell'informativa completa di secondo livello, che non corrisponde all'indirizzo sul quale, come dichiarato dal Comune, tale informativa sarebbe stata effettivamente pubblicata (v. all.ti 2 e 3 alla nota prot. n. XX del XX).

Quanto all'informativa sul trattamento dei dati di secondo livello, deve evidenziarsi che, nonostante la richiesta dell'Autorità di fornire copia delle diverse versioni di tale informativa succedutesi nel tempo, specificando per ciascuna versione la data di pubblicazione sul predetto sito (v. nota dell'XX, cit.), il Comune ha dichiarato di non essere in grado di recuperare tali documenti e che l'informativa, la cui prima versione risalirebbe al mese di luglio del XX, sarebbe stata successivamente modificata nelle seguenti date: “XX, XX, XX, XX e XX”. Con nota prot. n. XX del XX, il Comune ha depositato in atti il testo dell'ultima versione dell'informativa del XX (v. all. 6 alla nota alla nota prot. n. XX del XX), ovvero un documento pubblicato in data successiva a quella della prima richiesta d'informazioni rivolta al Comune (v. la citata nota dell'Autorità prot. n. XX del XX).

Quanto alla circostanza che il testo dell'informativa di secondo livello fosse comunque a disposizione degli interessati presso la sede del Comune, deve osservarsi che l'art. 12, par. 1, del Regolamento prevede che l'informativa di cui all'art. 13 del Regolamento debba essere "facilmente accessibile" agli interessati. A tal riguardo, il Comitato europeo per la protezione dei dati ha affermato che "le informazioni di secondo livello devono 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., par. 117). Ciò, tuttavia, sul presupposto che tale snodo centrale si trovi in prossimità della zona soggetta a videosorveglianza. Diversamente, allorquando i dispositivi di videosorveglianza siano distribuiti in maniera diffusa su un'ampia area geografica, ovvero, come nel caso di specie, sull'intero territorio comunale, l'informativa di primo livello deve rimandare necessariamente a un'informativa di secondo livello reperibile online, in maniera tale che gli interessati possano facilmente accedere alla stessa, senza doversi fisicamente recare presso la sede del titolare del trattamento, cosa che determinerebbe un effetto disincentivante e richiederebbe agli interessati uno sforzo che non può ritenersi proporzionato a quello minimo che, invece, sopporterebbe il titolare per la pubblicazione online del testo dell'informativa.

Né può accogliersi la tesi difensiva prospettata dall'Ente a scioglimento delle riserve formulate in sede di audizione, ovvero che i file di log del proprio sistema informatico comproverebbero la pubblicazione online sul proprio sito web di taluni documenti afferenti ai profili di protezione dei dati relativi all'impiego di dispositivi video, tra cui l'"informativa sistemi di videosorveglianza del territorio comunale". Ciò in quanto, non essendo il Comune riuscito a recuperare copia di tali documenti, non è possibile appurare il contenuto degli stessi, al fine della verifica del rispetto di quanto previsto dagli artt. 5, par. 1, lett. a), 12 e 13 del Regolamento.

Alla luce delle considerazioni che precedono, deve concludersi che il Comune non ha comprovato di aver fornito agli interessati un'informativa completa sul trattamento dei dati, di secondo livello, nel periodo intercorrente tra la data di attivazione dei propri dispositivi di videosorveglianza e il XX, avendo, pertanto, lo stesso agito in violazione degli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento.

Quanto al testo dell'informativa di secondo livello, pubblicata online a partire dal XX, deve rilevarsi che lo stesso, menzionando contestualmente più finalità di trattamento, senza specificare quali dispositivi video (con l'indicazione della relativa aree soggetto a videosorveglianza) siano utilizzati per perseguire ciascuna distinta finalità di trattamento, non consente agli interessati di essere debitamente informati in merito alle effettive finalità di trattamento perseguite caso per caso. In particolare, occorre rilevare che la finalità di trattamento connessa al "controllo dell'abbandono di rifiuti" non può essere perseguita con le medesime telecamere di videosorveglianza che riprendono ad ampio raggio la pubblica via per finalità di sicurezza urbana, potendo, invece, gli Enti locali utilizzare dispositivi video (c.d. fototrappole) collocati in specifiche e circoscritte aree, su cui insiste un effettivo rischio di illecito abbandono di rifiuti o scorretto conferimento degli stessi, a condizione che tali aree siano debitamente segnalate con cartelli informativi (in maniera tale che gli interessati abbiano piena contezza del fatto di essere ripresi e possano, se del caso e ove possibile, decidere di sottrarsi alla videosorveglianza) e solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi; ciò comunque nel rispetto del principio di minimizzazione dei dati, che impone di configurare tali dispositivi con un angolo di visuale circoscritto alle aree interessate dai predetti fenomeni, tipicamente caratterizzate da scarsa o limitata presenza umana (cfr. FAQ del Garante in materia di videosorveglianza, cit., n. 13. Pertanto, l'informativa in questione avrebbe dovuto specificare che tale finalità di trattamento si riferiva esclusivamente alle "2 telecamere a sorveglianza delle isole ecologiche", indicando chiaramente le specifiche aree su cui insistono le stesse (v. comunicato stampa del Comune menzionato in premessa), dovendosi, comunque, osservarsi che la l. 9 ottobre 2023, n. 137, di

conversione del d.l. 10 agosto 2023, n. 105, ha modificato l'art. 255 del d.lgs. 3 aprile 2006, n. 152, attraendo all'area penale talune condotte rilevanti in materia di tutela ambientale, prima sanzionate in via amministrativa.

L'informativa menziona, inoltre, una finalità di trattamento del tutto generica ("adempimento di oneri di legge") e non fa alcun riferimento alle finalità amministrative, perseguite dall'Ente, connesse alla verifica dell'assolvimento degli obblighi in materia di revisione e assicurazione obbligatoria di cui al Codice della Strada, non essendo indicati i cinque dispositivi video - con i relativi siti d'installazione - utilizzati per tali finalità di trattamento (v. art. 13, par. 1, lett. c), del Regolamento).

Deve, pertanto, concludersi che, anche successivamente al XX e fino alla data in cui i dispositivi video in questione sono stati disattivati, il Comune ha agito in violazione dell'art. 13, par. 1, lett. c), del Regolamento.

### **3.3 La valutazione d'impatto sulla protezione dei dati.**

In caso di rischi elevati per gli interessati - derivanti, ad esempio, dall'utilizzo di nuove tecnologie e sempre presenti laddove sia effettuata una sorveglianza sistematica su larga scala di una zona accessibile al pubblico (v. art. 35, par. 3, lett. c), del Regolamento) - il titolare del trattamento deve effettuare una valutazione d'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).

Nel caso di specie, il Comune era certamente soggetto all'obbligo di redigere una valutazione d'impatto sulla protezione dei dati, considerato che, ai sensi dell'art. 35, par. 3, lett. c), del Regolamento, la valutazione d'impatto è sempre richiesta in caso di "sorveglianza sistematica su larga scala di una zona accessibile al pubblico", circostanza che ricorre nel caso in esame, stante l'impiego di dispositivi video installati sulla pubblica via, di cui alcuni, peraltro, dotati di funzionalità di lettura automatizzate delle targhe dei veicoli in transito.

Ciò chiarito, si osserva che il Comune ha dichiarato che "la redazione della valutazione d'impatto è iniziata il XX e perfezionata a seguito delle implementazioni realizzate con gli interventi finalizzati in data XX e recepiti dal Regolamento Videosorveglianza approvato con Delibera n. XX del XX".

Premesso che, nel periodo intercorrente tra il 25 maggio 2018 (data di efficacia del Regolamento) e il XX, il Comune ha riconosciuto di non aver redatto una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del Regolamento, deve, in ogni caso, osservarsi che il documento depositato in atti dal Comune, contenente la predetta valutazione d'impatto, è privo di data certa, recando soltanto un'indicazione temporale del tutto generica ("anno XX"), peraltro incongruente rispetto all'asserita finalizzazione del documento in data XX. Al riguardo, il Comune ha dichiarato di non essere in possesso di "atti formali di ricevimento della [valutazione d'impatto]", redatta da un professionista da esso incaricato, non avendo, pertanto, l'Ente comprovato in maniera certa la data in cui sarebbe stata redatta la valutazione d'impatto sulla protezione dei dati depositata in atti. Tale documento risulta, peraltro, sottoscritto con firma autografa dal "progettista", ovvero un soggetto esterno all'organizzazione del titolare del trattamento, e non, invece, dal Sindaco, quale legale rappresentante dell'Ente, o da altro soggetto da questi formalmente delegato.

Alla luce delle considerazioni che precedono, non avendo il Comune comprovato di aver redatto una valutazione d'impatto sulla protezione dei dati in data certa anteriore a quella di avvio del trattamento, sottoscritta dal Sindaco o da altro soggetto formalmente delegato, deve concludersi che il Comune ha agito in violazione dell'art. 35 del Regolamento.

### **4. Conclusioni.**

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice, seppure meritevoli di considerazione, non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano insufficienti a consentire l'archiviazione del presente procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Si confermano, pertanto, le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato dal Comune, per aver trattato dati personali, mediante dispositivi video, in violazione degli artt. 5, par. 1, lett. a), 6, 12, par. 1, 13 e 35 del Regolamento del Regolamento, nonché 2-ter del Codice.

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, 6, 12, par. 1, e 13 del Regolamento, nonché 2-ter 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, come dichiarato nel corso dell'istruttoria, il Comune, ancorché non avesse ricevuto alcuna prescrizione in tal senso da parte dell'Autorità, ha spontaneamente ritenuto opportuno disattivare i dispositivi video in questione dopo aver ricevuto la contestazione di violazione amministrativa e, pertanto, prima di presentare le proprie memorie difensive - 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:

ancorché il Comune abbia raccolto i dati relativi alle targhe dei veicoli in transito per un esteso arco temporale, potendo così astrattamente ottenere informazioni delicate relative agli spostamenti degli interessati sul territorio comunale, l'Ente non ha trattato gli stessi nell'ambito dei procedimenti amministrativi di propria competenza, avendo soltanto conservato i numeri di targa per far fronte a eventuali richieste dell'Autorità giudiziaria o delle

Forze dell'Ordine nell'ambito delle indagini di loro competenza; l'Ente ha, dunque, agito con l'intento di servire un interesse pubblico, seppur, in maniera colposa, nell'erronea convinzione che sussistesse un idoneo quadro giuridico di settore a supporto dell'iniziativa intrapresa (art. 83, par. 2, lett. a) e b), del Regolamento);

sebbene il Comune non abbia comprovato la data certa della valutazione d'impatto sulla protezione dei dati, lo stesso ha comunque dichiarato di essersi avvalso di un consulente esperto ai fini della redazione di tale documento, che sarebbe stata comunque effettuata nel corso dello sviluppo e implementazione del progetto (art. 83, par. 2, lett. a), del Regolamento);

il trattamento ha riguardato un elevato numero di interessati e si è protratto per un esteso arco temporale (art. 83, par. 2, lett. a), del Regolamento);

non risulta in atti che specifici interessati abbiano subito un pregiudizio derivante dai trattamenti di dati personali posti in essere dal Comune con i dispositivi in questione (art. 83, par. 2, lett. a), 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 medio (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 piccole dimensioni (circa 5.131 abitanti), dotato, pertanto, di limitate risorse organizzative ed economiche e precisato che non può essere valorizzata, con valore attenuante, la circostanza, pure invocata dal Comune in sede di audizione, che l'Ente ha agito nel contesto dell'emergenza epidemiologica da SARS-CoV-2, atteso che il trattamento che ha avuto luogo per un esteso arco temporale e si è concluso ben oltre la cessazione del periodo di emergenza, si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze attenuanti:

il Comune ha offerto una buona cooperazione con l'Autorità nel corso dell'istruttoria, avendo, peraltro, spontaneamente interrotto il trattamento dei dati personali in questione dopo aver ricevuto la contestazione di violazione amministrativa notificatagli dall'Autorità (art. 83, par. 2, lett. f), del Regolamento);

non risultano precedenti violazioni pertinenti commesse dal Comune (art. 83, par. 2, lett. e), del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 4.000 (quattromila) per la violazione degli artt. 5, 6, 12, par. 1, 13 e 35 del Regolamento, nonché 2-ter del Codice, 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 ha riguardato i dati relativi alle targhe dei veicoli in transito sul territorio comunale, informazioni queste particolarmente delicate, atteso che, ancorché dall'istruttoria è emerso che il Comune si è limitato ad effettuare la sola conservazione degli stessi, dalla loro analisi possono essere astrattamente ottenute informazioni relative agli spostamenti degli

interessati sul territorio comunale, nonché tenuto conto che il trattamento ha avuto luogo per un esteso arco temporale.

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 Levanto per violazione degli artt. 5, 6, 12, par. 1, 13 e 35 del Regolamento, nonché 2-ter del Codice, nei termini di cui in motivazione;

### **ORDINA**

al Comune di Levanto, in persona del legale rappresentante pro-tempore, con sede legale in Piazza Cavour, 1 - 19015 Levanto (SP), C.F. 00197500119, di pagare la somma di euro 4.000 (quattromila) 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 4.000 (quattromila) 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 dinnanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

*Roma, 19 dicembre 2024*

IL PRESIDENTE  
Stanzione

IL RELATORE  
Cerrina Feroni

IL VICE SEGRETARIO GENERALE  
Filippi