Provvedimento del 18 dicembre 2025 [10213486]

[doc. web n. 10213486]

Provvedimento del 18 dicembre 2025

Registro dei provvedimenti
n. 752 del 18 dicembre 2025

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

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

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

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

VISTA la documentazione in atti;

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

RELATORE il prof. Pasquale Stanzione;

PREMESSO

1. Introduzione.

Con reclamo presentato ai sensi dell'art. 77 del Regolamento, XX ha lamentato di aver ricevuto un verbale di accertamento di violazione dell'art. 180, lett. d), del d.lgs. 30 aprile 1992, n. 285, Codice della Strada (di seguito, CdS), relativo all'obbligo di assicurazione dei veicoli, a seguito di un controllo effettuato mediante un dispositivo video utilizzato dal Comune di Nave (di seguito, il

Comune).

In particolare, è stato rappresentato che il Comune si è dotato di “un portale di lettura targhe, con installazione nel senso di marcia uscente dal paese, di una telecamera che provvedere a leggere automaticamente la targa di tutti i veicoli in transito”, che “i dettagli del transito (numero di targa, data ed ora, varco) vengono memorizzati dal sistema e [sono] disponibil[i] per successivi eventuali accertamenti” e che “il sistema di memorizzazione prevede una cancellazione automatica dei dati trascorsi 7 giorni dal transito”.

La reclamante ha, infine, lamentato di aver esercitato, con una nota del XX, il diritto di cancellazione dei propri dati personali ai sensi dell’art. 17 del Regolamento e di non aver ricevuto alcuna risposta da parte del Comune.

2. L’attività istruttoria.

Nel corso dell’istruttoria l’Autorità ha rivolto al Comune alcune richieste d’informazioni (v. note prot. nn. XX del X, XX del XX, XX del XX, XX del XX). Il Comune ha fornito riscontro alle stesse (v. note prot. nn. XX del XX, XX del XX, XX del XX, XX del XX), rendendo talune dichiarazioni, come riprese in prosieguo nella parte motiva del presente provvedimento.

Con nota del XX (prot. n. XX), l’Ufficio, sulla base degli elementi acquisiti, dalle verifiche compiute e dei fatti emersi a seguito dell’attività istruttoria, ha notificato al Comune, ai sensi dell’art. 166, comma 5, del Codice, l’avvio del procedimento per l’adozione dei provvedimenti di cui all’art. 58, par. 2, del Regolamento, per aver posto in essere un trattamento di dati personali, mediante dispositivi video, in maniera non conforme al principio di “liceità, correttezza e trasparenza” e in assenza di un’idonea base giuridica, in violazione dell’art. 5, par. 1, lett. a) e 6 del Regolamento, nonché 2-ter del Codice; omesso di assicurare la necessaria trasparenza del trattamento nei confronti degli interessati, in violazione degli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento; omesso di svolgere una valutazione di impatto sulla protezione dei dati, in violazione dell’art. 35 del Regolamento; omesso di fornire riscontro all’istanza di esercizio dei diritti presentata dall’interessata, in violazione degli artt. 12, parr. 3 e 4, 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, prospettando argomenti difensivi, ripresi in prosieguo nella parte motiva del presente provvedimento, poi sostanzialmente ribaditi in occasione dell’audizione, richiesta ai sensi dell’art. 166, comma 6, del Codice e tenutasi in data XX (v. verbale prot. n. XX della medesima data).

3. Esito dell’attività istruttoria.

3.1. La liceità del trattamento.

Il trattamento di dati personali mediante dispositivi video, da parte di soggetti pubblici, è generalmente ammesso se esso 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. artt. 5, par. 1, lett. a), 6, parr. 1, lett. c) ed e), 2 e 3, del Regolamento, nonché 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).

Con le citate note di riscontro alle richieste d’informazioni formulate dall’Autorità, il Comune ha dichiarato, in particolare, che:

l’Ente utilizza un “sistema di lettura targhe automatico […] che permette la connessione automatica con i database della Motorizzazione Civile per la verifica in tempo reale della copertura assicurativa, della revisione periodica e della classe ambientale dei veicoli in transito”;

“il sistema […] non [rileva] i dati personali del proprietario del veicolo transitante; sarà cura dell’operatore di polizia stradale effettuare una ricerca completa se necessaria ai fini della contestazione di una eventuale sanzione riguardante un veicolo segnalato dal sistema”;

“è un sistema non omologato per l’accertamento a distanza delle infrazioni ma costituisce un semplice “supporto” per la documentazione della violazione che è stata comunque accertata dall’operatore di polizia stradale”;

“nel caso prospettato l’operatore che stava monitorando il transito dei veicoli ha ricevuto un alert di segnalazione per il veicolo della segnalante che, transitando sotto il varco lettura targhe, ha attivato uno dei sistemi di controllo (mancanza assicurazione, revisione, classe ambientale)”;

“non è stata immediatamente contestata l’infrazione ex art 193/2° del [CdS] (circolazione con veicolo sprovvisto di assicurazione) al proprietario del veicolo in quanto a volte è successo che a seguito di alert positivo si accertava invece che il veicolo segnalato avesse attivato l’assicurazione da poco e che l’archivio della MCTC non fosse ancora aggiornato. Si è proceduto quindi ad emettere un verbale ex art 180 del [CdS], senza sanzione pecuniaria, invitando il proprietario del veicolo a fornire informazioni in merito all’obbligo di assicurazione del veicolo. Solo a seguito di mancata presentazione di quanto richiesto e dopo aver fatto ulteriori controlli si è accertato che il veicolo circolava sprovvisto di assicurazione obbligatoria verso terzi”;

“il sistema […] è stato installato nel Comune […] nel dicembre del XX […]”;

il sistema […] è continuativamente attivo e permette all’operatore di Polizia Locale di monitorare gli illeciti di cui sopra ogni qualvolta ci si colleghi al software; i transiti dei veicoli segnalati rimangono comunque in memoria per 7 giorni, indipendentemente dal loro monitoraggio”;

“dal XX […il sistema è stato] utilizzato solo come strumento di ausilio per la contestazione immediata delle violazioni di cui agli artt. 193 e 80 del C.d.S. Infatti, la pattuglia in servizio si posiziona a debita distanza dal rilevatore targhe e tramite l’ausilio di un dispositivo che si collega al sistema, ricevendo in tempo reale un alert di segnalazione, ferma il veicolo e contesta immediatamente l’infrazione, dopo aver effettuato un ulteriore controllo documentale”;

“solo nel caso [in cui] non si riesca a fermare il veicolo in transito, per oggettivi impedimenti (ad es. perché si ha già un veicolo fermo per la contestazione), viene effettuata la contestazione successiva degli artt. 193 e 80 del C.d.S. Non vengono inviati verbali ex art. 180 del C.d.S., ed i veicoli sanzionati sono solo quelli che effettivamente transitano avanti al posto di controllo”;

“il sistema […], oltre al monitoraggio dei veicoli sprovvisti di assicurazione e revisione è stato altresì predisposto per il censimento delle classi ambientali dei veicoli in transito. Questa funzionalità è stata attivata in quanto era un requisito indispensabile per accedere alle sovvenzioni regionali per l’acquisto della strumentazione”;

“come previsto dal bando Regione Lombardia, D.d.s. XX n. XX […] l’Ente beneficiario del contributo si impegna a trasmettere [alla] Regione […], periodicamente e sistematicamente per tre anni successivi all’attivazione degli impianti, i dati dei flussi di traffico e la relativa caratterizzazione per classe ambientale dei veicoli”;

“il Comune […] ha partecipato al bando ed è stato ammesso al cofinanziamento […] e sta trasmettendo i flussi veicolari, con cadenza semestrale, come da istruzioni pervenute in data XX […]”;

“la base giuridica del trattamento dei dati è finalizzata a scopi di interesse pubblico [art. 6 (1) e) GDPR] e per l’accertamento di alcune infrazioni (comprese il transito di veicoli maggiormente inquinanti) che, senza l’ausilio di determinate apparecchiature elettroniche, sarebbe difficoltoso, se non impossibile, effettuare. Controlli quindi che si possono effettuare tramite impianti di rilevazione elettronica come previsto dall’art 13, comma 6 bis della L.R. Lombardia n. 24/06 e dall’art 201, comma 1 bis del D.lgs 285/92 (Nuovo Codice della Strada)”;

“la rilevazione della classe ambientale dei veicoli […] costituisce un trattamento di un dato tecnico relativo alle caratteristiche del veicolo la cui finalità risiede in provvedimenti adottati dalla Regione Lombardia a cui sono demandate le norme in materia di tutela dell’ambiente che vengono di seguito indicate: la legge regionale 11 dicembre 2006, Norme per la prevenzione e la riduzione delle emissioni in atmosfera a tutela della salute e dell’ambiente; legge regionale 29 giugno 2009, Legge regionale 6 agosto 2019, n. 15, la quale ha l’obiettivo di assicurare una più efficace tutela della salute e dell’ambiente, nonché per prevenire infrazioni comunitarie in materia di inquinamento atmosferico. Tale norma tenuto conto dello stato di qualità dell’aria e al fine di irrogare le sanzioni amministrative previste dall’articolo 27, consente l’utilizzo di impianti di rilevazione elettronica”;

“[…] la Regione Lombardia sono stati trasmessi esclusivamente informazioni che non contengono dati personali relativi ai veicoli che sono transitati dai portali di rilevazione dei transiti”;

“il processo di anonimizzazione dei dati implementato dall’algoritmo di rilevazione dei transiti è il seguente: la lavorazione dei dati avviene tramite procedura automatica in apposita sezione “Report” del programma […]. I dati salvati sono solo quelli relativi al numero di transiti e alla relativa direzione associati ad ogni varco, i dati soggetti a privacy (targa, proprietario…) vengono cancellati automaticamente dal sistema al termine dei giorni di privacy impostati (7 gg) e rimangono in memoria, tramite apposito algoritmo, solo il numero di veicoli transitanti diviso per categoria ambientale e solo quest’ultimi dati vengono trasmessi a Regione Lombardia”;

“attualmente sono installate n. 103 telecamere”;

“vi sono inoltre n. 3 telecamere di lettura targhe (Varchi) che utilizzano il sistema [… in oggetto];

“attualmente il Comune [la] non ha stipulato alcun patto per la sicurezza urbana con la Prefettura di Brescia”.

A partire dal XX, il Comune ha, pertanto, installato numerose telecamere, di cui tre dotate di un

sistema di lettura automatizzata delle targhe dei veicoli in transito, connesso con le banche dati della Motorizzazione Civile, per la verifica in tempo reale della copertura assicurativa, della revisione periodica e della classe ambientale dei veicoli in transito, trasmettendo alcuni dati in forma anonima semestralmente alla Regione Lombardia, nonché ha dichiarato di perseguire finalità di sicurezza urbana, pur non avendo stipulato alcun patto per l'attuazione della sicurezza urbana con la Prefettura territorialmente competente.

Sul punto, si osserva che la normativa di settore, vigente all'epoca dei fatti oggetto di reclamo, disciplina la possibilità di accertare alcune violazioni al CdS attraverso appositi dispositivi video, nel rispetto di alcune condizioni (cfr. artt. 45, 193, comma 4-ter, 198, 198-bis, 201, commi 1-bis, lett. e), f), g), g-bis) e g-ter) del CdS). Al fine di assicurare il rispetto dei principi di "liceità, correttezza e trasparenza", "minimizzazione" e "limitazione della conservazione" (art. 5, par. 1, lett. a) c) ed e) del Regolamento), gli apparecchi di rilevazione:

> per essere utilizzati per il rilevamento da remoto delle violazioni di cui agli artt. 80 e 193 CdS con contestazione differita, devono essere gestiti direttamente dagli organi di polizia stradale e devono fungere da mero supporto di documentazione della violazione, dovendosi, di regola, procedere sempre alla contestazione immediata, salvo che specifiche situazioni di fatto, da attestarsi nel verbale, rendano impossibile la contestazione immediata (cfr. la circolare del Ministero dell'interno del XX, prot. n. XX in materia di "Contestazione differita delle violazioni di cui agli artt. 80 e 193 del Codice della Strada");
>
> pur potendo effettuare un continuo monitoraggio del traffico, nell'arco temporale in cui è presente una pattuglia in loco, devono essere configurati in modo da memorizzare dati personali solo in caso di effettiva infrazione al CdS (cfr. la circolare del Ministero dell'interno del XX, prot. XX, ancorché relativa ai sistemi di rilevamento della velocità; in giurisprudenza, v. Consiglio di Stato, sez. V, sent. 18 gennaio 2021, n. 509; cfr. provv. 19 dicembre 2024, n. 805, doc. web n. 10107263).

Viceversa, come è emerso dall'istruttoria, i dispositivi video in questione, privi di omologazione, non venivano attivati soltanto negli intervalli temporali in cui agenti della Polizia locale si trovavano fisicamente presenti in prossimità delle aree sottoposte a controllo ai fini della contestazione immediata delle violazioni, ma erano in funzione su base continuativa, raccogliendo e conservando per sette giorni tutti i dati relativi ai veicoli in transito, indipendentemente dall'effettivo accertamento di una violazione delle predette disposizioni del CdS.

Quanto al perseguimento, mediante i dispositivi video installati sul territorio comunale, della finalità di tutela della c.d. sicurezza urbana, deve osservarsi quanto segue. La disciplina di settore consente ai Comuni l'installazione di sistemi 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 compente, che, nel caso di specie, non ha avuto luogo (v. artt. 4 e 5, co. 2, lett. a), del d.l. 20 febbraio 2017, n. 14; v. già l'art. 6, co. 7 e 8, del d.l. 23 febbraio 2009, n. 11; cfr. provv.ti 4 dicembre 2025, n. 730, in corso di pubblicazione;13 novembre 2025, n. 669, doc. web n. 10198694; 23 ottobre 2025, n. 628, doc. web n. 10196164; 10 aprile 2025, n. 201, doc. web n. 10139433; 19 dicembre 2024, n. 805, doc. web n. 10107263; 20 giugno 2024, n. 374, doc. web n. 10028498; 11 gennaio 2024, n. 5, doc. web n. 9977020; 20 ottobre 2022, n. 341, doc. web n. 9831369).

Non può, a tal riguardo, accogliersi la tesi prospettata dall'Ente in sede di memoria difensiva, secondo la quale "[i patti per l'attuazione della sicurezza urbana] sono facoltativi e non obbligatori, [essendo] compito comunque primario del Sindaco (Autorità locale di pubblica sicurezza) mettere in atto tutte quelle misure finalizzate alla sicurezza dei propri cittadini ed una di quelle è appunto il monitoraggio del territorio grazie alla videosorveglianza, considerato il numero esiguo di agenti di polizia locale in dotazione dell'ente". L'art. 5, commi 1 e 2, del d.l. 20 febbraio 2017, n. 14, ha,

infatti, ricondotto “l'installazione di sistemi di videosorveglianza” per la “prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria” all’alveo degli “interventi per la sicurezza urbana” da individuarsi “con appositi patti sottoscritti tra il prefetto ed il sindaco”. Come evidenziato dal Ministero dell’interno con propria circolare (N. XX del XX), anche “a seguito degli interventi normativi che sono stati ricordati e della susseguente elaborazione giurisprudenziale compendiata negli interventi spesso “ortopedici” della Consulta [v., in particolare, sent. 196/2009 e 226/2010], [in merito al] concetto di sicurezza urbana” e “al di là della distinzione tra sicurezza primaria e sicurezza secondaria [… si] vede consolidarsi l’ambito oggettivo della prima [, tanto] che l’interessamento del Comitato provinciale per l’ordine e la sicurezza pubblica finisce col diventare, anche in un’ottica di potenziamento della sicurezza integrata, una stabile modalità di valutazione degli apparati di videosorveglianza nell’ambito comunale”. Da qui l’impostazione del legislatore del 2017 di subordinare la possibilità per i Comuni di impiegare sistemi di videosorveglianza sul proprio territorio, finalizzati alla prevenzione e al contrasto dei fenomeni di criminalità diffusa e predatoria, alla previa stipula di un patto per l’attuazione della sicurezza urbana con la Prefettura territorialmente competente. I patti in questione non riguardano, peraltro, unicamente i sistemi di videosorveglianza realizzati in maniera integrata tra comuni e autorità di pubblica sicurezza, non rinvenendosi alcuna indicazione in tal senso nell’art. 5, comma 2, lett. a), del d.l. 20 febbraio 2017, n. 14. (cfr., da ultimo, l’art. 2 del patto tipo predisposto dal Ministero dell’interno e allegato alla circolare n. XX delXX, che fa riferimento ai “progetti anche integrati dei sistemi di videosorveglianza” e dunque non solo a questi). D’altra parte, lo stanziamento di fondi pubblici in favore dei Comuni “ai fini dell'installazione di sistemi di videosorveglianza” è previsto espressamente per i sistemi “di cui al comma 2, lettera a)” (art. 5, co. 2-ter del, 20 febbraio 2017, n. 14) e, dunque, a quelli oggetto di uno specifico patto tra Sindaco e Prefettura territorialmente competente (cfr., da ultimo, l’art. 2, comma 2, del decreto del Ministero dell’interno del XX, adottato di concerto con il Ministero dell’Economia e delle Finanze, ai sensi del quale “possono produrre richiesta per accedere al “finanziamento” i comuni […] che hanno sottoscritto i “patti” che individuano come prioritario obiettivo, per la prevenzione e il contrasto dei fenomeni di criminalità diffusa e predatoria, l’installazione di sistemi di videosorveglianza in determinate zone del territorio comunale o infra-comunale”, non essendo previsto che i progetti finanziabili siano soltanto quelli di videosorveglianza c.d. integrata).

La mancata stipula di un patto per l’attuazione della sicurezza urbana non consente, pertanto, di ricondurre i trattamenti di dati personali in questione alla disciplina di settore di cui all’art. 5, co. 2, lett. a), del d.l. 20 febbraio 2017, n. 14.

In disparte da ogni considerazione in merito all’idoneità di tale disciplina di settore a giustificare l’impiego da parte di comuni di dispositivi video, peraltro non omologati, di dispositivi video dotati di funzionalità di lettura automatizzata dei veicoli in transito, la medesima conclusione vale anche in merito ai tre dispositivi video utilizzati dal Comune nel caso di specie, stante la mancata stipula di un patto per l’attuazione della sicurezza urbana con la Prefettura territorialmente competente (cfr. provv.ti 4 dicembre 2025, n. 730, in corso di pubblicazione; 19 dicembre 2024, n. 805, doc. web n. 10107263).

Per quanto concerne, invece, il trattamento dei dati relativi ai transiti veicolari per finalità statistiche e la comunicazione degli stessi in forma aggregata alla Regione Lombardia, deve, anzitutto, ribadirsi che il Comune non ha comprovato la sussistenza di un’idonea base giuridica che potesse giustificare il trattamento di tali dati per le finalità di trattamento originarie (sicurezza urbana; accertamento di violazioni di disposizioni del CdS). La circostanza che il bando della Regione prevedesse il finanziamento dell’acquisito di dispositivi per la rilevazione e il controllo automatico delle targhe dei veicoli in transito è, peraltro, irrilevante, atteso che i dispositivi in questione non sono stati impiegati dal Comune, come invece previsto da detto bando (v. parere della Regione Lombardia prodotto in allegato alla menzionata nota del XX), per il controllo degli accessi a zone a traffico limitato o soggette a disposizioni di limitazione della circolazione per motivi ambientali,

bensì per la diversa finalità di controllo dell'assolvimento degli obblighi previsti dal CdS in materia di revisione e assicurazione obbligatoria, nonché per finalità di sicurezza urbana.

Da tutto quanto sopra emerge, peraltro, su un piano più generale, una sostanziale e perdurante difficoltà dell'Ente, in quanto titolare del trattamento, a tenere distinte le varie finalità di trattamento perseguite e a individuare con chiarezza per ciascuna di essere una specifica disposizione di settore che possa costituire la base giuridica del trattamento. Anche in sede di memoria difensiva, il Comune ha, infatti, fatto riferimento a una pluralità di finalità di trattamento, che esso intende perseguire mediante i dispositivi video in questione, tra loro estremamente eterogenee e che non trovano puntuale in disposizioni idonee per rango e qualità a disciplinare il trattamento (tutela della pubblica sicurezza e della sicurezza urbana; polizia giudiziaria; vigilanza sull'osservanza di ordinanze o regolamenti comunali; protezione civile; accesso a zone a traffico limitato e corsie riservate; monitoraggio della circolazione stradare; tutela del patrimonio; tutela ambientale e controllo del conferimento dei rifiuti; accertamento delle violazioni amministrative in materia di circolazione stradale; statistica).

Alla luce delle considerazioni che precedono, deve concludersi che, utilizzando sul proprio territorio dispositivi video in questione, di cui tre dotati di funzionalità di lettura automatizzata dei numeri di targa dei veicoli in transito, il Comune ha posto in essere un trattamento di dati personali in maniera non conforme al principio di liceità, correttezza e trasparenza e in assenza di un'idonea base giuridica, in violazione degli artt. 5, par. 1, lett. a), e 6, parr. 1, lett. c) ed e), 2 e 3, del Regolamento, nonché 2-ter del Codice.

3.2. La trasparenza nei confronti degli interessati.

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

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" del Comitato europeo per la protezione dei dati, adottate il 29 gennaio 2020, 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. le FAQ del Garante in materia di videosorveglianza, doc. web n. 9496574, 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 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. 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, in riscontro alle richiamate richieste d'informazioni rivoltegli dall'Autorità, il Comune ha dichiarato che:

- "gli impianti di video sorveglianza installati sul territorio del Comune […] sono stati segnalati […mediante] cartelli segnaletici […]. L[a] informativ[a] di dettaglio […era] pubblicat[a] sul sito internet del comune nella sessione privacy [… in forma] generica […]. Recentemente è stata adottata e pubblicata la nuova informativa specifica in materia di videosorveglianza";

- "il Comune […] ha assolto agli obblighi informativi in merito al trattamento dei dati personali tramite la pubblicazione delle informative sul sito www.comune.nave.bs.it nella pagina PRIVACY/informative con [la] pubblicazion[e] del […] XX (informativa videosorveglianza)";

Quanto all'informativa di primo livello, il Comune, pur avendo dichiarato di aver installato dei cartelli informativi in prossimità delle aree soggette a videosorveglianza, non è stato in grado di indicare la data a partire della quale gli stessi sarebbero stati installati. In sede di memoria difensiva, l'Ente ha ammesso "che [il] cartello [contenente l'informativa di primo livello] risulta mancante di alcuni dettagli informativi […]" e ha dichiarato di aver "già sostituito alcuni cartelli riportanti le informazioni di primo livello (dal XX) […]", nonché di aver "predisposto un piano di adeguamento dell'intera cartellonistica […]".

Il cartello contenente l'informativa di primo livello (all. XX nota del XX, prot. n. XX), presente al momento dei fatti oggetto di reclamo, non risulta, infatti, pienamente conforme ai requisiti previsti dalla normativa in materia di protezione dei dati personali, in quanto esso indica riferimenti non aggiornati in merito alla normativa sulla protezione dei dati personali (v. 5, par. 1, lett. a) e art. 12, par. 1, del Regolamento); non menziona i dati di contatto del responsabile della protezione dei dati (v. art. 13, par. 1, lett. b), del Regolamento); non indica la totalità delle finalità perseguite e la relativa base giuridica (v. art. 13, par. 1, lett. c), del Regolamento); non specifica i tempi di conservazione dei dati (v. art. 13, par. 2, lett. a), del Regolamento); non menziona compiutamente i diritti degli interessati di cui agli artt. 15 e seg. del Regolamento e le modalità di esercizio degli stessi (v. art. 13, par. 2, lett. b), del Regolamento); non specifica le modalità attraverso le quali gli interessati possono accedere a un'informativa completa di secondo livello (v. 5, par. 1, lett. a) e art. 12, par. 1, del Regolamento).

Quanto all'informativa completa di secondo livello, il Comune ha dichiarato che, alla data della rilevazione della sanzione comminata alla reclamante, non aveva pubblicato un'informativa specifica per gli impianti di videosorveglianza, poiché "erroneamente si pensasse bastasse la pubblicazione dell'informativa generale sul trattamento dei dati che include più servizi e non specificatamente quello della videosorveglianza". In sede di memoria difensiva, l'Ente ha riconosciuto che "[…] l'informativa di dettaglio (secondo livello) […] non era presente nel momento della contestazione".

Il Comune ha poi provveduto a pubblicare tale informativa soltanto in data XX, successivamente all'avvio dell'istruttoria da parte dell'Autorità. Pertanto, fino a tale data, il Comune non ha fornito agli altri interessati un'informativa completa, di secondo livello, sul trattamento dei dati personali raccolti e trattati con i dispositivi video in questione.

Deve, inoltre, rilevarsi che anche l'informativa sul trattamento dei dati personali "relativa all'impianto di videosorveglianza e di controllo targhe veicoli", pubblicata sul sito web istituzionale del Comune a partire dal XX (v. all. XX alla nota prot. n. XX del XX), non risulta comunque pienamente conforme ai requisiti previsti dalla normativa in materia di protezione dei dati personali, in quanto:

- vengono menzionate finalità di trattamento ulteriori rispetto a quelle dichiarate dal Comune nel corso dell'istruttoria e tra loro eterogenee, senza che sia indicata la specifica disciplina di

settore che, ad avviso del Comune, costituirebbe la base giuridica del trattamento e che espressamente consentirebbe l'impiego di dispositivi video sul territorio comunale per il perseguimento delle stesse; ciò con particolare riguardo alle seguenti finalità: "attivare misure di tutela della pubblica sicurezza, la prevenzione, accertamento o repressione dei reati svolti sul territorio comunale"; "vigilare […] sulla corretta osservanza di ordinanze e/o regolamenti comunali per consentire l'accertamento dei relativi illeciti"; "vigilare sul traffico e consentire la ricostruzione della dinamica degli incidenti stradali, nonché monitorare la circolazione stradale al fine di intervenire prontamente per prevenire ingorghi o blocchi del traffico"; "attivare uno strumento operativo a supporto delle attività di protezione civile sul territorio comunale"; "tutelare il patrimonio comunale e privato per la prevenzione e repressione di atti vandalici o di teppismo in luoghi pubblici"; "monitorare le aree usate come discariche abusive per l'accertamento e la repressione di comportamenti illeciti e reati ambientali, oltre che al monitoraggio del corretto utilizzo delle piazzole ecologiche per il conferimento dei rifiuti"; "acquisire prove e filmati nell'ambito dell'attività di indagini di polizia giudiziaria" (v. art. 13, par. 1, lett. c), del Regolamento);

non si fa comunque alcuna menzione dei trattamenti posti in essere al fine di rilevare la classe dei veicoli inquinanti e ottenere i dati statistici comunicati alla Regione Lombardia (v. art. 5, par. 1, lett. a), 12, par. 1, e 13, par. 1, lett. c), del Regolamento), avendo l'Ente a tal riguardo dichiarato in sede di memoria difensiva che e che "si provvederà ad aggiornare la stessa indicando la rilevazione della classe ambientale del veicolo e la base giuridica e si provvederà a distinguere le finalità relative all'informativa tra impianti di contesto e impianti relativi alla lettura delle targhe".

Alla luce delle considerazioni che precedono, deve concludersi che il Comune ha fornito agli interessati un'informativa di primo livello non idonea, nonché, fino al XX, ha omesso di fornire l'informativa estesa di secondo livello sul trattamento dei dati personali. A partire dal XX, lo stesso ha, invece, fornito agli interessati un'informativa completa di secondo livello non pienamente conforme ai requisiti previsti dalla normativa in materia di protezione dei dati, avendo, pertanto, agito in violazione degli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento.

3.3. La valutazione di 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 di impatto sulla protezione dei dati, al fine di adottare, in particolare, le misure adeguate ad affrontare tali rischi, consultando preventivamente il Garante (v. artt. 35 e 36, par. 1, del Regolamento), qualora dalla valutazione di impatto emerga che il rischio residuante non possa essere ragionevolmente attenuato (cfr. cons. 94 del Regolamento; cfr. le "Linee guida in materia di valutazione di impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679", adottate dal Gruppo di lavoro art. 29 il 4 ottobre 2017, WP 248 rev.01, e poi fatte proprie dal Comitato europeo per la protezione dei dati con "Endorsement 1/2018" del 25 maggio 2018, ove si evidenzia che "ogniqualvolta il titolare del trattamento non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati) è necessario consultare l'autorità di controllo").

Sul punto il Comune ha dichiarato nel corso dell'istruttoria di "non [aver] ritenuto [di dover] svolgere una valutazione di impatto [sulla protezione dei dati] in quanto ha ritenuto i rischi, relativi agli interessati, contenuti, trattandosi di una tecnologia consolidata e avendo affidato la realizzazione ad una ditta qualificata che ha attuato misure di sicurezza per la protezione dei dati".

Si osserva, tuttavia, che 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 stessa è sempre richiesta in caso di “sorveglianza sistematica su larga scala di una zona accessibile al pubblico”, circostanza che ricorre nel caso di specie.

In sede di memoria difensiva, il Comune ha dichiarato che “provvederà a sviluppare la valutazione di impatto anche per gli impianti di video sorveglianza installati sul territorio, sia per le telecamere di contesto che per i tre varchi posizionati sul territorio del comune di Nave” e che tale attività era stata “avviata prima della data del reclamo [….], ma non conclusa in quanto si voleva provvedere ad aggiornare i cartelli informativi e ad adeguare l'intero impianto a modelli di sicurezza più congrui prima di renderla definitiva”, così confermando che la valutazione di impatto sulla protezione dei dati non era stata svola prima dell’avvio del trattamento mediante i dispositivi video in questione, con la conseguente violazione dell’art. 35 del Regolamento.

3.4 L’istanza di esercizio del diritto di cancellazione dei dati

L’art. 12 del Regolamento prevede che il titolare del trattamento debba fornire all'interessato le informazioni relative all’azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 del Regolamento senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa (par. 3). Se non ottempera alla richiesta dell’interessato, il titolare del trattamento deve informare l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale (par. 4). Ne deriva che il titolare del trattamento, in ottemperanza agli obblighi di trasparenza, è tenuto a fornire riscontro anche se sussistono dei ragionevoli motivi per non poter accogliere l’istanza nel merito.

Nel caso in esame la reclamante ha lamentato di aver esercitato, con una nota del XX, il diritto di cancellazione dei propri dati personali, ai sensi dell’art. 17 del Regolamento, e di non aver ricevuto alcun riscontro da parte del Comune.

Al riguardo, il Comune, in riscontro alle richieste di chiarimento dell’Ufficio, ha dichiarato di non aver dato riscontro all’interessata in merito all’istanza di cancellazione dei dati “in quanto non applicabile per via dei procedimenti in essere e all’obbligo previsto dalla norma di conservazione dei dati”.

L’Ente non ha, pertanto, informato l’interessata “dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale” (art. 12, par. 4, del Regolamento).

In sede di memoria difensiva, l’Ente ha, d’altra parte, ammesso che “la procedura attivata dal Titolare non è stata conforme al modo di operare solito dell'ufficio di Polizia Locale e ai contenuti dell'art. 12 del reg UE 2016/679” e che “a tale fine è stata predisposta una procedura per la corretta gestione delle istanze degli utenti e a sensibilizzare gli uffici in tal senso”.

La condotta dell’Ente si pone, pertanto, in violazione degli artt. 12, parr. 3 e 4, 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, parr. 1, lett. c) ed e), 2 e 3, 12, parr. 1, 3, 4, 13 e 35 del Regolamento, nonché 2-ter del Codice.

La violazione delle predette disposizioni rende applicabile la sanzione amministrativa prevista dall'art. 83, par. 5, del Regolamento, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 3, del Regolamento medesimo, come richiamato anche dall'art. 166, comma 2, del Codice.

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).

In tale quadro, si prende atto delle dichiarazioni rese dal Comune nel corso del procedimento in ordine alla disattivazione, a partire dal XX, dei "tre varchi di lettura targhe siti sul Comune […] sono stati disattivati nella funzione continua di rilevazione dei transiti veicolari" (v. nota del XX, prot. n. XX).
Tenuto conto che sul territorio comunale sono tutt'ora presenti circa cento telecamere di videosorveglianza, si ritiene necessario ingiungere all'Ente, ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, di (i) effettuare una ricognizione di tutte le telecamere di videosorveglianza presenti sul proprio territorio e di appurare, quali tra queste siano effettivamente strumentali al perseguimento della finalità di tutela della sicurezza urbana, provvedendo conseguentemente a stipulare accordi con le competenti Autorità di pubblica sicurezza; (ii) stabilire le eventuali ulteriori finalità di trattamento perseguite mediante i medesimi dispositivi video, rinvenendo un'idonea base giuridica che possa giustificare il trattamento per ciascuna di tali finalità; (iii) svolgere o adeguare la valutazione di impatto sulla protezione dei dati personali; (iv) rivedere le informative sul trattamento dei dati personali di primo e di secondo livello rese agli interessati.

Ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, il Comune dovrà 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 ingiunto ai sensi del citato art. 58, par. 2, lett. d), del Regolamento.

Tenuto conto del tempo trascorso non risulta, invece, possibile adottare provvedimenti correttivi in relazione alle violazioni relative alle disposizioni del Regolamento che disciplinano l'esercizio dei diritti dell'interessato.

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).

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, 13 del Regolamento e 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.

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, la violazione ha carattere colposo, essendo stata posta in essere per effetto di errate valutazioni sul piano giuridico da parte dell'Ente (art. 83, par. 2, lett. a) e b), del Regolamento);

- alla Regione Lombardia sono stati messi a disposizione unicamente dati statistici e aggregati, che non consentono di risalire all'identità degli interessati (art. 83, par. 2, lett. a), del Regolamento);

- non risulta dalla documentazione in atti che la reclamante, nel contesto dell'istanza di cancellazione dei propri dati personali, abbia subito ulteriori pregiudizi per effetto del mancato riscontro da parte dell'Ente (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 limitate dimensioni (circa 10.662 abitanti), si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze:

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

- il titolare, nonostante le evidenziate perduranti difficoltà nel conformarsi pienamente alla disciplina di protezione dei dati, ha offerto una sufficiente cooperazione con l'Autorità (art. 83, par. 2, lett. f) del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 6.000 (seimila) per la violazione degli artt. 5, par. 1, lett. a), 6, parr. 1, lett. c) ed e), 2 e 3, 12, parr. 1, 3, 4, 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.

In tale quadro 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 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, senza assicurare la necessaria trasparenza nei confronti degli interessati e senza aver effettuato una valutazione di impatto sulla protezione dei dati.

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 degli artt. 57, par. 1, lett. f), del Regolamento, l'illiceità del trattamento effettuato dal Comune di Nave per violazione degli artt. 5, parr. 1, lett. a), 6, parr. 1, lett. c) ed e), 2 e 3, 12, parr. 1, 3 e 4, 13 e 35 del Regolamento, nonché 2-ter del Codice, nei termini di cui in motivazione;

ORDINA

al Comune di Nave, in persona del legale rappresentante pro-tempore, con sede legale in via Paolo VI, n. 17 - 25075 Nave (BS), C.F. 80008790174, di pagare la somma di euro 6.000 (seimila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione. Si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

al predetto Comune:

- di pagare la complessiva somma di euro 6.000 (seimila) in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, secondo le modalità indicate in allegato, entro trenta giorni dalla notifica 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 (i) effettuare una ricognizione di tutte le telecamere di videosorveglianza presenti sul proprio territorio e di appurare, quali tra queste siano effettivamente strumentali al perseguimento della finalità di tutela della sicurezza urbana, provvedendo conseguentemente a stipulare accordi con le competenti Autorità di pubblica sicurezza; (ii) stabilire le eventuali ulteriori finalità di trattamento perseguite mediante i medesimi dispositivi video, rinvenendo un'idonea base giuridica che possa giustificare il trattamento per ciascuna di tali finalità; (iii) svolgere o adeguare la valutazione di impatto sulla protezione dei dati personali; (iv) rivedere le informative sul trattamento dei dati personali di primo e di secondo livello rese agli interessati;

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

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 del Garante;

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, 18 dicembre 2025

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Montuori