

The background of the poster is a photograph of a historic Italian town square. On the left, a white church with a tall brick bell tower is visible. On the right, a large, ornate brick building with multiple levels of arched windows and a crenellated roofline stands. In the foreground on the right, there is a large, detailed stone statue of a standing figure, possibly a saint or historical figure, mounted on a tiered pedestal. The sky is a clear, bright blue.

GROSSETO | 2 e 3 OTTOBRE 2025

Teatro degli Industri

3° CONVEGNO DI STUDI PER LA POLIZIA LOCALE E SICUREZZA URBANA

Santo Fabiano



La peculiarità dell'attività di vigilanza territoriale



Finalità, convivenze, interferenze e complessità

- ◆ La sicurezza pubblica
- ◆ La tutela ambientale e del patrimonio
- ◆ La tutela della riservatezza
- ◆ L'esercizio dei diritti
- ◆ Il rispetto delle prescrizioni normative
- ◆ Le competenze istituzionali



1. occorre chiarire gli scopi che si intendono perseguire e verificare se sono leciti in base alle norme vigenti: se l'attività è svolta, ad esempio, per prevenire pericoli concreti o specifici reati, occorre rispettare le competenze che le leggi assegnano per tali fini solo a determinate amministrazioni pubbliche;
2. il trattamento dei dati deve avvenire per scopi determinati, espliciti e legittimi;
3. i soggetti che sono tenuti a notificare al Garante l'esistenza di banche dati devono indicare fra le modalità di trattamento anche la raccolta di informazioni mediante apparecchiature di videosorveglianza;
4. i cittadini devono essere informati, in maniera chiara anche se sintetica, della presenza di telecamere e dei diritti che possono esercitare sui propri dati, tanto più se le apparecchiature non sono immediatamente visibili;
5. per il controllo a distanza dei lavoratori rimangono comunque validi i divieti e le garanzie previsti dallo Statuto dei lavoratori;
6. i dati raccolti devono essere quelli strettamente necessari agli scopi perseguiti: vanno pertanto registrate solo le immagini indispensabili, va limitato l'angolo visuale delle riprese, vanno evitate immagini dettagliate o ingrandite e, di conseguenza, vanno stabilite in maniera adeguata la localizzazione delle telecamere e le modalità di ripresa;
7. va stabilito con precisione entro quanto tempo le immagini devono essere cancellate e occorre prevedere la loro conservazione solo in relazione a illeciti che si siano verificati o a indagini giudiziarie o di polizia;
8. vanno individuate, **con designazione scritta, le persone che possono utilizzare gli impianti e prendere visione delle registrazioni** e deve essere vietato l'accesso alle immagini ad altri soggetti, salvo che si tratti di indagini giudiziarie o di polizia;
9. i dati raccolti per determinati fini (ad esempio sicurezza, tutela del patrimonio) non possono essere utilizzati per finalità diverse o ulteriori (ad esempio per pubblicità, analisi dei comportamenti di consumo), fatte salve le esigenze di polizia o di giustizia e non possono essere diffusi o comunicati a terzi;
10. le immagini registrate per la rilevazione degli accessi dei veicoli ai centri storici devono rispettare l'apposito regolamento (D.P.R. 250/1999) ed essere conservate per il solo periodo necessario alla contestazione delle infrazioni.

01/09/22, 12:39

about:blank



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Ordinanza ingiunzione nei confronti di Comune di Policoro - 9 giugno 2022 [9794895]

[doc. web n. 9794895]

Ordinanza ingiunzione nei confronti di Comune di Policoro - 9 giugno 2022

Registro dei provvedimenti
n. 214 del 9 giugno 2022

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



In particolare, il reclamante ha rappresentato di aver ricevuto tre verbali di accertamento, con i quali venivano irrogate sanzioni amministrative per aver “abbandonato i rifiuti solidi urbani” in data XX, XX e XX.

L'accertamento delle violazioni, mediante visione delle immagini di videosorveglianza, sarebbe, tuttavia, avvenuto rispettivamente in data XX (ovvero 82 giorni dopo la data della registrazione delle immagini), XX (ovvero 79 giorni dopo la data della registrazione delle immagini) e XX (ovvero 64 giorni dopo la data della registrazione delle immagini).

Il reclamante ha, altresì, lamentato l'inidonea installazione dei cartelli contenenti l'informativa semplificata sulla videosorveglianza, nonché la non conformità dell'informativa contenuta nei verbali notificatogli dal Comune, in quanto “carente del contenuto prescritto dagli artt. 13 e 14 del Regolamento [e contraddistinta da genericità con riguardo] alla specifica finalità di accertamento compiuto”.

Infine, il reclamante ha rappresentato di aver provveduto “ad incardinare innanzi all'Ufficio del Giudice di Pace di XXX tre distinti giudizi [...], con i quali, opponendosi alle sanzioni irrogate [dal Comune], contestava l'illegittima acquisizione ed utilizzazione dei dati personali e richiedeva la condanna dell'Amministrazione al risarcimento dei danni”.

Nell'ambito di tali giudizi, il Comune si sarebbe costituito con il patrocinio di un avvocato che risulta essere anche il Responsabile della protezione dei dati (“RPD”) del Comune. Per tale ragione, è stata lamentata una situazione di “incompatibilità fra il [RPD] e l'incarico di difesa del Comune, tenuto conto che il [RPD] è intervenuto in un procedimento in cui si evidenziavano le illegittimità nel trattamento dei dati”.

3.2 I principi di “limitazione della conservazione” e “responsabilizzazione”.

Ai sensi dell'art. 5, par. 1, lett. e), del Regolamento, i dati personali devono essere “conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati” (“limitazione della conservazione”).

In base al principio di responsabilizzazione (artt. 5, par. 2, e 24 del Regolamento), spetta al titolare del trattamento individuare i tempi di conservazione delle immagini, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche; ciò salvo che specifiche norme di legge non prevedano espressamente specifici tempi di conservazione dei dati.

Anche con riguardo ai trattamenti di dati personali effettuati mediante sistemi di videosorveglianza, le immagini registrate non possono essere conservate più a lungo di quanto necessario per le finalità per le quali sono acquisite. In particolare, “i dati personali dovrebbero essere – nella maggior parte dei casi (ad esempio se la videosorveglianza serve a rilevare atti vandalici) – cancellati dopo pochi giorni, preferibilmente tramite meccanismi automatici.

Quanto più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione”.



Nel corso dell'attività istruttoria, è emerso che il Comune non ha fissato i tempi massimi di conservazione delle immagini riprese mediante le c.d. fototrappole ai fini del contrasto al fenomeno dell'illecito abbandono dei rifiuti e, conseguentemente, con riguardo al caso oggetto di reclamo, ha proceduto all'accertamento delle violazioni amministrative in tempi superiori a due mesi rispetto alla data di registrazione delle immagini.

Anche in relazione a tale profilo, il **Comune ha sostenuto che i trattamenti di dati personali da esso effettuati sarebbero da ricondursi ad attività di polizia giudiziaria, con conseguente applicazione del d.lgs. 18 maggio 2018, n. 51. Tali tesi non può, tuttavia, trovare accoglimento, valendo, a tal riguardo, le considerazioni sopra esposte in merito alla piena applicazione delle disposizioni del Regolamento e del Codice ai trattamenti di dati personali effettuati dal Comune ai fini dell'accertamento di violazioni amministrative in materia ambientale.**

Di conseguenza, nell'ottica del principio di responsabilizzazione e in ossequio al principio di limitazione della conservazione, il Comune avrebbe dovuto definire i termini massimi di conservazione delle immagini di videosorveglianza per ciascuna finalità di trattamento perseguita, motivando adeguatamente le scelte a tal riguardo compiute.

Pertanto, il Comune ha trattato dati personali mediante dispositivi video in maniera non conforme ai principi di "limitazione della conservazione" e "responsabilizzazione", in violazione degli artt. 5, par. 1, lett. e), e par. 2 (in combinato disposto con l'art. 24) del Regolamento.



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Provvedimento del 4 giugno 2025 [10163530]

[doc. web n. 10163530]

Provvedimento del 4 giugno 2025

Registro dei provvedimenti
n. 322 del 4 giugno 2025

... il titolare del trattamento deve adottare misure appropriate per fornire all'interessato tutte le informazioni in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (art. 12, par. 1, del Regolamento).

In particolare, 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".

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".

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.

La segnaletica di avvertimento di primo livello deve contenere inoltre un chiaro riferimento al secondo livello di informazioni, ad esempio indicando un sito web sul quale è possibile consultare il testo dell'informativa estesa.

Si evidenzia inoltre che, per il perseguimento della finalità di trattamento connessa al controllo degli illeciti amministrativi in materia ambientale gli Enti locali possono utilizzare dispositivi foto/video (c.d. fototrappole) collocati in specifiche e circoscritte aree su cui insiste un effettivo rischio di illecito abbandono di rifiuti o scorretto conferimento di rifiuti, solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi, e dovendo comunque agire 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.

Nel corso dell'istruttoria è emerso che il trattamento risulta essere stato effettuato dal Comune in violazione del principio di "liceità, correttezza e trasparenza" di cui all'art. 5, par. 1, lett a) e dell'obbligo che impone al titolare del trattamento di rendere agli interessati una preventiva informativa, secondo quanto previsto dagli artt. 12 e 13 del Regolamento.

Ciò in quanto al momento dei fatti, **non era presente sul luogo sottoposto a videosorveglianza alcun cartello informativo volto a rendere edotta l'interessata** – e gli ulteriori soggetti ripresi - in merito ai trattamenti effettuati mediante dispositivi foto/video ai fini dell'accertamento dello scorretto conferimento dei rifiuti urbani, atteso che gli stessi erano stati temporaneamente rimossi rispetto all'area di ripresa di tali dispositivi; **in aggiunta, nell'informativa di primo livello inizialmente fornita agli interessati – sebbene rimossa all'epoca dei fatti oggetto di reclamo - mancava un chiaro riferimento al secondo livello di informazioni fornito sul sito web istituzionale del Comune.**



Per quanto concerne gli aggiornamenti effettuati dal Comune in corso d'istruttoria, deve evidenziarsi che, alla luce della documentazione prodotta in atti, **nell'informativa di primo livello risultano tuttora indicate una pluralità di finalità**, sebbene il sistema foto/video finalizzato ad accertare lo scorretto conferimento di rifiuti urbani sia stato strutturato in modo da avere una "[...] differenziazione della tipologia dei mezzi di ripresa, distinguendo quelli [...] specifici per monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente, [...] il cui] angolo di ripresa è stato verificato in modo da minimizzare la zona sorvegliata, circoscritta alla specifica funzione sopra richiamata [...]".

La medesima pluralità di finalità si riscontra, altresì, nell'informativa di secondo livello, reperibile sul sito web istituzionale del Comune.



Si rappresenta, inoltre, che, nella predetta informativa di secondo livello è indicato che "Ai sensi e per gli effetti di cui all'articolo 6 del GDPR, La informiamo che **la base giuridica a sostegno del trattamento dei Suoi dati personali è rappresentata dalla necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il titolare del trattamento (art. 6 par. 1 lettera e) oltre che dalla necessità di perseguire un **legittimo interesse del titolare del trattamento quale desumibile dalle sopra indicate** finalità (art. 6 par. 1 lettera f)".

Sul punto, si ricorda che ai sensi di quanto previsto dall'art. 6, par. 1 del Regolamento, **il legittimo interesse "non si applica al trattamento dei dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti"**, posto che "spetta al legislatore prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati personali". Pertanto, essendo il Comune un soggetto pubblico, la base giuridica del legittimo interesse non può trovare applicazione in relazione ai trattamenti posti in essere dallo stesso.

Deve, inoltre, considerarsi:

- che non risultano comprovati eventuali danni subiti dagli interessati (art. 83 par. 2, lett. a) del Regolamento);
- il carattere colposo della violazione (art. 83, par. 2, lett. b) del Regolamento);
- che i trattamenti in questione non sono relativi a categorie particolari di dati (art. 83, par. 2, lett. g).

Alla luce di tali circostanze, si ritiene che, nel caso di specie, il livello di gravità della violazione commessa dal titolare del trattamento possa essere considerato di grado medio.

Ciò premesso, si ritiene che, ai fini della quantificazione della sanzione, debba essere presa in considerazione, in senso favorevole, che il titolare del trattamento è un Comune di modeste dimensioni e che:

- non risultano precedenti violazioni pertinenti commesse dal titolare del trattamento (art. 83, par. 2, lett. e), del Regolamento);
- il grado di cooperazione manifestato dal titolare con l'autorità di controllo al fine di provare a porre rimedio alla violazione e attenuarne i possibili effetti negativi, (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 5.000,00 (cinquemila/00) per la violazione degli artt. 5, par. 1, lett. a) e c), 12, par. 1 e 13, parr. 1 e 2 del Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Provvedimento del 27 marzo 2025 [10138999]

[doc. web n. 10138999]

Provvedimento del 27 marzo 2025

Registro dei provvedimenti
n. 168 del 27 marzo 2025

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



Con reclamo presentato in data XX ai sensi dell'art. 77 del Regolamento, il sig. XX ha lamentato una presunta violazione della disciplina in materia di protezione dei dati personali, riguardante la ricezione di un verbale di contestazione dell'infrazione dell'art. 7, comma 14, del del D.Lgs. 30 aprile 1992, n. 285 ("Nuovo Codice della Strada", o "C.d.S.") accertata mediante sistema di videosorveglianza, per aver acceduto in un'area ZTL in assenza della relativa autorizzazione.

In particolare, il reclamante ha rappresentato la **poca chiarezza nell'individuazione del titolare del trattamento** in quanto, nella cartellonistica presente all'epoca dei fatti, era indicato il Comune di XXX in luogo del Nuovo Circondario XXX, con conseguente pregiudizio in merito al principio di trasparenza anche ai fini del corretto esercizio dei diritti da parte degli interessati.

- "Con la Convenzione per la gestione associata della funzione di polizia locale (approvata dal Comune di Imola con deliberazione C.C. n. XX del XX e dal NCI con deliberazione dell'Assemblea n. XX del XX), in vigore dal XX [...] il Comune di XXX ha conferito le funzioni comprendenti tutti i compiti e le attività di polizia locale definiti dalla L. 65/1986 e dalla L.R. 24/2003, ivi compresa la videosorveglianza e il fotocontrollo degli accessi, al Nuovo Circondario XXX [...]"
- per quanto concerne l'informativa di primo livello "Nella segnaletica installata in prossimità dei varchi non era stato registrato il mutato assetto istituzionale a far data dal XX e, pertanto, figurava il Comune di XXX quale Titolare del trattamento", il cui aggiornamento "è stato effettuato il XX";



Con riferimento alla condotta del Nuovo Circondario XXX, l'Ufficio, sulla base degli elementi acquisiti e dei fatti emersi a seguito dell'attività istruttoria, ha notificato allo stesso, in data XX (prot. n. XX) 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 agito in maniera non conforme al principio di "liceità, correttezza e trasparenza" e per **aver provveduto a redigere la valutazione d'impatto sulla protezione dei dati successivamente all'avvio del trattamento dei dati personali**, in violazione degli artt. 5, par. 1, lett. a), 12, 13 e 35 del Regolamento.

Nel corso dell'istruttoria è emerso che dalla data del 1° gennaio XX (in cui è subentrato a seguito di una Convenzione per la gestione associata della funzione di polizia locale al Comune di Imola nella gestione delle funzioni comprendenti tutti i compiti e le attività di polizia locale compresa la videosorveglianza e il controllo degli accessi), al XX, il Nuovo Circondario XXX **non ha provveduto ad aggiornare l'informativa di primo livello, ed in particolare il riferimento al nuovo titolare del trattamento, né a pubblicare l'informativa di secondo livello sul proprio sito istituzionale**, operando pertanto in violazione del principio di "liceità, correttezza e trasparenza" (art. 5, par. 1, lett. a) del Regolamento) nonché degli artt. 12 e 13 del Regolamento.

Per quanto concerne, invece, il contestato mancato svolgimento della valutazione d'impatto sulla protezione dei dati prima dell'avvio del trattamento dei dati personali (art. 35 del Regolamento), preso atto di quanto dichiarato dal Nuovo Circondario XXX in corso d'istruttoria in relazione alle peculiarità del sistema di "fotocontrollo implementato, [...consistente in] un impianto omologato protetto e isolato, [...] separato e distinto dal sistema di videosorveglianza", il quale ai fini della rilevazione e registrazione delle immagini dei veicoli che accedono all'area Ztl senza permesso autorizzativo, fotografa la targa dei veicoli in transito non censiti in apposita whitelist - contenente l'elenco delle targhe autorizzate ad entrare nell'area ZTL - e non persone o altri veicoli, si dispone, alla luce degli specifici elementi emersi nel caso concreto, l'archiviazione della contestazione della violazione dell'art. 35 del Regolamento.



| **GPDP** |

**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



L'Autorità ha appreso da un articolo di stampa che il Comune di XXX 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.



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”.



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 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”;

[...]

“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”



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. 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, 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**".



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 XXX"), 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"), 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).

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**