GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Provvedimento del 4 luglio 2024

[doc. web n. 10050298]

Provvedimento del 4 luglio 2024

Registro dei provvedimenti
n. 405 del 4 luglio 2024

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 cons. Fabio Mattei, segretario generale;

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

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

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

Vista la documentazione in atti;

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

Relatore il dott. Agostino Ghiglia;

PREMESSO

1. Introduzione.

Da un articolo di stampa si è appreso che il Comune di Treviso (di seguito, il "Comune") avrebbe impiegato droni provvisti di dispositivi video in grado di individuare fonti di calore, inclusi i corpi umani, al fine di contrastare il fenomeno dei furti notturni nelle abitazioni.

Nel medesimo articolo si faceva, inoltre, riferimento alla possibilità per i cittadini di segnalare eventuali reati subiti attraverso un'applicazione informatica denominata "TrevisoSicura".

2. L'attività istruttoria.

In riscontro a una richiesta d'informazioni dell'Autorità, il Comune, con nota del 7 dicembre 2022 (prot. n. 0180056/2022), come integrata con note del 22 febbraio 2023, ha dichiarato, in particolare, che:

A) in riferimento all'impiego dei droni da parte della Polizia locale:

- "all'interno del Comando della Polizia Locale […] è stato costituito un nucleo specializzato di agenti, volto all'impiego della specifica tecnologia rappresentata dagli APR (aeromobile a pilotaggio remoto) più comunemente conosciuti con il termine di "droni"";

- "tutti gli APR hanno pay load costituiti da apparati fotografici con ottiche idonee all'ottenimento di scatti fotografici e registrazioni video, [e taluni sono] dotati di opzione termica";

- "le ottiche a infrarossi, o telecamere termiche, fanno riferimento a strumenti tecnologici che, basandosi sulla rilevazione, senza contatto, del calore emesso da un qualsiasi oggetto o corpo che abbia una temperatura superiore allo zero assoluto (-273.15 C°), sotto forma di raggi infrarossi, invisibili quindi a occhio nudo, ne elabora l'immagine, restituendo all'operatore che ha in uso detti supporti, l'avvistamento di cose nella totale o semi oscurità, potendone generare poi una foto o video";

- "[…] l'immagine, visualizzata sul visore dell'operatore di polizia o sul monitor dell'operatore SAPR, corrisponde alla mappa di calore che l'oggetto, o il soggetto, emanante produce. Il segnale termico è convertito in elettrico e quindi la scena viene riportata su uno schermo come se fosse un'immagine televisiva";

- "gli APR, fino alla data della richiesta di informazioni da parte dell'Autorità, hanno trovato impiego […] [, tra le altre cose,] nelle operazioni di polizia e pubblica sicurezza per le quali la Polizia Locale viene coinvolta in ragione delle sue funzioni e competenze ausiliarie ai sensi dell'art. 5 L. 65/86";

- "l'uso delle tecnologie citate non prevede che soggetti possano essere in qualche modo identificati o identificabili poiché queste hanno il solo scopo di rendere visibili all'operatore "mappe di calore", costituite da sagome indistinguibili che poi vengono segnalate agli operatori di polizia locale che, in coordinamento con la centrale operativa, opportunamente guidati, eseguono poi l'accertamento di polizia "di persona" con la classica identificazione di polizia e l'eventuale excursus giudiziario o amministrativo";

- "[…] nessuna attività di catalogazione o raccolta o trattamento dati viene eseguita, e non è stata mai eseguita attraverso l'uso di dette tecnologie, nemmeno con il rilievo di temperature espresse in gradi celsius, poiché le termocamere restituiscono solo variazioni di colori in relazione alle variazioni di temperature rilevate, ma non rivelano il dato "temperatura" del soggetto da utilizzare in via esclusiva nella ricerca di soggetti dispersi nell'ambito degli interventi in caso di calamità naturali";

- "[…] dal giorno in cui si è venuti a conoscenza della richiesta di informazioni da parte dell'Autorità Garante, si è sospesa, in via preventiva e cautelativa, qualsiasi forma di utilizzazione dei droni".

B) in riferimento all'applicazione "TrevisoSicura":

- "l'APP denominata "TrevisoSicura" è fornita dalla Società Lapis [sas] [di seguito, la "Società"] […]";

- "il Comando di PL attraverso le segnalazioni che pervengono volontariamente dai cittadini riceve specifiche e circostanziate segnalazioni relative a rifiuti abbandonati sul territorio comunale […]";

- "la stessa APP permette ai cittadini di segnalare di aver subito un furto e il luogo dove si è consumato: questo permette all'ufficio di polizia giudiziaria del comando di PL di meglio individuare le zone colpite da reati predatori per poi organizzare servizi mirati sia in borghese che in uniforme per

la prevenzione dei predetti reati. Si tratta di una normale attività di polizia giudiziaria, curata dagli agenti e Ufficiali di polizia giudiziaria";

- "altra modalità prevista dalla App riguarda la comunicazione verso il cittadino, avvisato della disponibilità di notizie dal Comune con la ricezione di una notifica";

- "la segnalazione richiede obbligatoriamente il nominativo e il numero di telefono del segnalante per poter procedere con la validazione della stessa tramite invio di un messaggio SMS da confermare tramite link. Successivamente il sistema procede con l'inoltro all'amministrazione";

- "è inoltre possibile […] allegare una foto o scattarla contestualmente";

- "è invece obbligatorio indicare la tipologia di segnalazione (rifiuti, furti, ecc.) e un campo messaggio a testo libero dove il cittadino può fornire ulteriori informazioni";

- "il personale di PL riceve una notifica via e-mail di nuova segnalazione e provvede ad inoltrare ai colleghi l'informazione per gli ulteriori accertamenti e la risoluzione della problematica evidenziata dal cittadino";

- "è evidente che tale modalità non correttamente strutturata a livello di processo, […] poteva […] provvisoriamente e in un primo momento assolvere all'esigenza di apertura di un canale di comunicazione verso i cittadini ma, evidentemente, necessita di una completa revisione";

- "la stessa modalità di trasferimento della segnalazione via e-mail è stato probabilmente l'elemento fuorviante, a partire dal fornitore che, secondo l'informativa pubblicizzata all'indirizzo web https://trevisosicura.it/privacy.html [...] riveste il ruolo di titolare, ponendo irritualmente i destinatari delle segnalazioni (enti locali e forze di polizia) addirittura come "Responsabili del trattamento", peraltro in evidente contrasto con quanto invece previsto dall'art. 2-ter del Codice";

- "la non corretta identificazione delle figure e il conseguente rovesciamento dei ruoli previsti dalla disciplina non ha soltanto formalmente viziato l'impianto generale ma anche i dovuti adempimenti, a partire dalla nomina a responsabile del trattamento e alla dovuta, quanto coerente rispetto al trattamento, informativa ai cittadini […]";

- "la app in oggetto, dopo un periodo sperimentale, è stata attivata dal 27.07.2020. Finora sono arrivate da parte dei cittadini una media di circa 400 segnalazioni annue, a fronte di un numero di download riportato nell'Android Store di più di 1.000 a partire dalla data di pubblicazione. Tuttavia, subito dopo la richiesta di informazioni da parte dell'Autorità Garante, le funzionalità di segnalazione sono state immediatamente disabilitate lasciando soltanto le eventuali notifiche delle news";

- "l'adozione della app da parte del Comune di Treviso ha l'obiettivo di migliorare e facilitare la comunicazione tra cittadini e amministrazione, considerando anche la modalità push di invio delle notifiche rispetto ad eventi, manifestazioni e notizie. Le segnalazioni da parte dei cittadini rientrano a pieno titolo nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri così come previsti a partire dal TUEL";

- "al momento il periodo di conservazione delle segnalazioni riportato nell'informativa è al massimo 12 mesi; nella pagina web della app è invece riportato un tempo di conservazione di 3 mesi dalla segnalazione con successiva cancellazione automatica. In considerazione della finalità e soprattutto della modalità di routing delle segnalazioni, si ritiene, al fine di ridurre considerevolmente la superficie di esposizione e conseguentemente i rischi per gli interessati, di evitare a monte tale conservazione da parte dei sistemi o comunque di limitare ad un numero di giorni compatibili con eventuali problematiche di ricezione della posta elettronica, aggiornando conseguentemente l'informativa";

- "[…] il fornitore della app deve essere nominato Responsabile del trattamento e [occorre] fornire allo stesso specifici requisiti tecnici e organizzativi in merito alla app stessa e alla sicurezza del back end […]";

- “al momento non sono stat[e] adottate determinazioni volte a disciplinare i trattamenti di dati personali derivanti dalla messa a disposizione della app dovute all’errata identificazione dei ruoli previsti dal Regolamento. Le uniche determinazioni riguardano l’attivazione/manutenzione del servizio per gli anni 2021 e 2022”.

Con nota del 6 aprile 2023 (prot. n. 0058164), 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, in relazione alle seguenti presunte violazioni della normativa in materia di protezione dei dati:

a) nel contesto dell’impiego dei droni:

- per aver trattato dati personali, anche relativi a reati, in maniera non conforme al principio di “liceità, correttezza e trasparenza”, in assenza di un idoneo presupposto normativo, in violazione degli artt. 5, par. 1, lett. a), 6 e 10 del Regolamento, nonché 2-ter e 2-octies del Codice;

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

b) nel contesto dell’impiego dell’applicazione informatica “TrevisoSicura”:

- per aver trattato i dati personali degli utenti dell’applicazione informatica in assenza di un’idonea base giuridica, in violazione degli artt. 5, par. 1, lett. a) e 6 del Regolamento, nonché 2-ter del Codice;

- per aver fornito agli interessati un’inidonea informativa sul trattamento dei dati personali, in violazione degli artt. 5, par. 1, lett. a), e 13 del Regolamento;

- per aver omesso di stipulare, in qualità di titolare del trattamento, un accordo sulla protezione dei dati con la Società, quale responsabile del trattamento, in violazione dell’art. 28, par. 3, del Regolamento;

- per aver agito in maniera non conforme ai principi di protezione dei dati fin dalla progettazione e per impostazione predefinita, nonché di responsabilizzazione, in violazione degli artt. 5, par. 2 (in combinato disposto con l’art. 24), e 25 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 4 maggio 2023 (prot. n. 0135761/23), il Comune ha presentato una memoria difensiva, dichiarando, in particolare, che:

- “l’impiego di droni [avviene] […] solamente per finalità amministrative e per attività che non prevedono trattamento di dati personali, se non in via eventuale o accidentale”;

- “[…] per le attività poste in essere di competenza della polizia locale, l’uso delle tecnologie citate non prevede il trattamento di dati personali e, a maggior ragione, [non è previsto] il trattamento dei dati giudiziari ai sensi dell’art. 10 [del Regolamento]”;

- “[…] non sono stati identificati soggetti nel corso dell’attività svolta da parte dei piloti dei droni e […] le prassi del titolare non prevedono alcun tipo di riconoscimento in tali condizioni”;

- “[…] l’utilizzo del drone con termo-camera, in attesa di avere indicazioni sul corretto utilizzo, è già stato sospeso […]”;

- “in riferimento all’app “TrevisoSicura” si conferma, purtroppo, [che l’iniziativa è] frutto di un affidamento in un periodo complicato come quello autunnale del 2020 [in cui] la necessità di tutelare la salute della popolazione […] risultava necessaria [e] espressamente richiesta da parte delle autorità

sanitarie";

- "[…] per contenere e rimediare agli errori commessi, si è proceduto a bloccare in data 25 novembre 2022 la possibilità per la cittadinanza di effettuare delle segnalazioni, […] a far levare l'informativa inserita, avendo reso l'applicazione, di fatto, inutilizzabile. Si è successivamente proceduto [alla rimozione] della app dagli store ove è pubblicata";

- "si è già provveduto a dismettere il rapporto con il fornitore, concluso contrattualmente il 31.12.2022, e la relativa app, al fine di procedere con una nuova assegnazione che sia conforme a tutti i principi di protezione dei dati indicati, partendo con un approccio conforme ai principi di privacy by design";

- "[…] solo in alcuni casi sono stat[e] comunicate delle situazioni che soltanto astrattamente potevano essere qualificat[e] come reati";

- "il numero di download della app corrispond[e] a circa l'1% della popolazione residente e […] il numero di segnalazioni totali nel periodo risulta estremamente limitato", essendo state ricevute n. "43" segnalazione relative a "buche e segnalazioni varie", n. "352" segnalazioni relative a "rifiuti" e n. "19" segnalazioni relative a "furti"".

In occasione dell'audizione, richiesta ai sensi dell'art. 166, comma 6, del Codice e tenutasi in data 13 dicembre 2023 (v. verbale prot. n. 0165047 del 13 dicembre 2023), il Comune ha dichiarato, in particolare, che:

- "l'articolo di stampa da cui ha avuto origine l'istruttoria dell'Autorità non riportava in maniera corretta le effettive modalità di utilizzo dei droni da parte del Comune";

- "a seguito dell'avvio dell'istruttoria da parte dell'Autorità, il Comune ha effettuato delle verifiche interne, da cui è emerso che i droni sono stati dotati di dispositivi fotografici soltanto per effettuare attività amministrativa";

- "non risulta che i droni siano stati utilizzati per finalità di polizia da parte del Comune, se non, in via residuale, su specifica richiesta delle Forze dell'Ordine, che hanno chiesto supporto alla Polizia locale per lo svolgimento di specifiche attività di polizia";

- "per quanto attiene all'applicazione, […] solo un numero limitato di utenti ha utilizzato l'applicazione (circa l'1% dei cittadini) e anche il numero di segnalazioni inviate tramite l'applicazione, rispetto a quelle che ordinariamente sono presentate alla Polizia locale, è contenuto. Pertanto, il trattamento ha avuto ad oggetto un ristretto novero di dati personali";

- "l'Ente aveva, peraltro, presentato l'applicazione anche in seno al Comitato Provinciale per l'Ordine e la Sicurezza Pubblica, che, in persona del Prefetto, aveva espresso apprezzamento per l'iniziativa".

3. Esito dell'attività istruttoria.

3.1. Il trattamento di dati personali mediante droni dotati di telecamere termiche

Preliminarmente occorre rilevare che, diversamente da quanto ritenuto dal Comune, l'impiego di droni dotati di telecamere termiche, al fine di generare c.d. mappe di calore, sulla base delle quali possono essere disposti controlli de visu da parte delle pattuglie della Polizia locale in servizio sul territorio, può comportare un trattamento di dati personali (cfr. artt. 2, par. 1, e 4 nn. 1 e 2, del Regolamento), anche relativi a reati (v. art. 10 del Regolamento e 2-octies del Codice). Com'è, infatti, emerso nel corso dell'istruttoria (v. filmati esemplificativi in atti), sebbene non sia possibile riconoscere il volto dei soggetti ripresi, le immagini permettono comunque di visualizzare, con un discreto livello di definizione, le sagome e i movimenti degli stessi. Si tratta, pertanto, comunque di informazioni che, a seguito dell'eventuale identificazione dei presunti autori dei reati da parte degli agenti della Polizia locale o delle Forze dell'ordine intervenuti sul luogo, possono essere associate a persone fisiche identificate ed essere utilizzate come elementi di prova di fattispecie di reato.

Deve poi evidenziarsi che, in attuazione dell'art. 5, comma 3-sexies, del d.l. 18 febbraio 2015, n. 7, l'art. 3 del decreto del Ministero dell'interno del 13 giugno 2022 prevede che "le Forze di polizia impiegano gli UAS [, sistemi di aeromobile senza equipaggio,] ai fini del controllo del territorio per finalità di ordine e sicurezza pubblica, con particolare riferimento al contrasto del terrorismo e alla prevenzione dei reati di criminalità organizzata e ambientale". Il quadro normativo di settore non consente, pertanto, in via generale alle Polizie locali dei Comuni di impiegare droni, dotati di dispositivi video, per finalità connesse alla tutela della pubblica sicurezza, fatti salvi i casi in cui funzioni ausiliari di pubblica sicurezza siano delegate alla Polizia locale dalle autorità competenti per specifiche operazioni (v. art. 3 e 5, comma 1, lett. c), della l. 7 marzo 1986, n. 65), in ogni caso nel rispetto delle condizioni previste dalla normativa di settore che disciplina l'impiego dei droni in tale contesto (cfr. art. 2, par. 3, lett. a) del regolamento (UE) 1139/2018; regolamento di esecuzione (UE) n. 947/2019; regolamento UAS-IT dell'Ente Nazionale per l'Aviazione Civile del 4 gennaio 2021, art. 2, par. 1, lett. b) e Sezione II - Parte B; artt. 743-746 e 748 del r.d. 30 marzo 1942, n. 327), la vigilanza sulla quale esula dalle competenze attribuite al Garante dalla normativa in materia di protezione dei dati.

Tuttavia, deve prendersi atto di quanto dichiarato dal Comune, con assunzione di responsabilità anche ai sensi dell'art. 168 del Codice, in merito alla circostanza che l'articolo di stampa, da cui è originata l'istruttoria, "non riportava in maniera corretta le effettive modalità di utilizzo dei droni da parte del Comune". L'Ente ha, altresì, dichiarato che a seguito di verifiche interne, "non risulta che i droni siano stati utilizzati per finalità di polizia da parte del Comune, se non, in via residuale, su specifica richiesta delle Forze dell'Ordine, che hanno chiesto supporto alla Polizia locale per lo svolgimento di specifiche attività di polizia". Inoltre, secondo quanto rappresentato dal Comune, "non sono stati identificati soggetti nel corso dell'attività svolta da parte dei piloti dei droni". Si ritiene, pertanto, che, in relazione ai trattamenti di dati personali in questione e con riguardo alle contestate violazione degli artt. 5, par. 1, lett. a), 6, 10 e 35 del Regolamento, nonché 2-ter e 2-octies del Codice, debba disporsi l'archiviazione del procedimento, non risultando comprovata, allo stato degli atti, una violazione della normativa in materia di protezione dei dati personali (v. art. 14 del Regolamento del Garante n. 1/2019).

3.2. Il trattamento di dati personali nel contesto dell'utilizzo dell'applicazione informatica "TrevisoSicura"

3.2.1. La liceità del trattamento

Nel corso dell'istruttoria è emerso che l'applicazione informatica "TrevisoSicura" non veniva utilizzata dagli utenti per presentare formalmente denunce di reato alla Polizia locale in funzione di polizia giudiziaria (con l'eventuale indicazione anche degli estremi dei presunti autori dei reati), essendo stata concepita unicamente come uno strumento attraverso il quale i cittadini potevano presentare generiche segnalazioni in merito a reati, non attribuiti a specifici soggetti considerati quali presunti autori, al fine di consentire alla Polizia locale di avere contezza, su base aggregata, delle zone della città maggiormente interessate da fenomeni criminali e organizzare "servizi mirati […] [di] prevenzione dei […] reati".

Di conseguenza, contrariamente a quanto sostenuto dal Comune nel corso dell'istruttoria, la Polizia locale del Comune non ha svolto in tale contesto una funzione di polizia giudiziaria.

Al riguardo, deve, infatti, osservarsi che la l. 7 marzo 1986, n. 65 (Legge quadro sull'ordinamento della polizia municipale) assegna al personale di polizia municipale lo svolgimento di quattro ordini di funzioni: di polizia locale (art. 1); di polizia giudiziaria (art. 5, lett. a)); di polizia stradale (art. 5, lett. b)); di pubblica sicurezza (art. 5, lett. c)).

L'art. 55 c.p.p. precisa che "1. La polizia giudiziaria deve, anche di propria iniziativa, prendere notizia dei reati, impedire che vengano portati a conseguenze ulteriori, ricercarne gli autori, compiere gli atti necessari per assicurare le fonti di prova e raccogliere quant'altro possa servire per l'applicazione della legge penale. 2. Svolge ogni indagine e attività disposta o delegata dall'autorità giudiziaria. 3. Le funzioni indicate nei commi 1 e 2 sono svolte dagli ufficiali e dagli agenti di polizia giudiziaria".

La Corte di Cassazione ha chiarito, con orientamento consolidato, che "ai sensi della L. 7 marzo 1986, n. 65, art. 5 e dell'art. 57 c.p.p., comma 2, lett. b), la qualità di agenti di polizia giudiziaria è espressamente attribuita alle guardie dei comuni, alle quali è riconosciuto il potere di intervento nell'ambito territoriale

dell'ente di appartenenza e nei limiti delle proprie attribuzioni, tra le quali rientra lo svolgimento di funzioni attinenti all'accertamento di reati di qualsiasi genere, che si siano verificati in loro presenza, e che richieda un pronto intervento anche al fine di acquisizione probatoria" (Cass. pen. Sez. III, Sent., ud. 07/06/2022, 30/08/2022, n. 31930; v. anche Cass. pen., sez. 1, 10/03/1994, n. 1193; in merito ai limiti territoriali della competenza di polizia giudiziaria degli agenti della Polizia locale, v. anche Cass. civ. Sez. II Ord., 08/02/2019, n. 3839; Cass. civ. Sez. VI - 2 Ord., 30/01/2019, n. 2748).

Pertanto, "la qualifica di agenti di polizia giudiziaria attribuita agli appartenenti alla polizia municipale è […] limitata nel tempo ("quando sono in servizio") e nello spazio ("nell'ambito territoriale dell'ente di appartenenza"), a differenza di altri corpi (Polizia di Stato, Carabinieri, Guardia di Finanza) i cui appartenenti operano su tutto il territorio nazionale e sono sempre in servizio" (v. Cass. civ. Sez. lavoro, Ord., 02/12/2019, n. 31388; Cass. pen. 10/06/2015, n. 35099).

Conseguentemente, le operazioni di polizia giudiziaria da parte della Polizia locale, d'iniziativa dei singoli durante il servizio, sono ammesse esclusivamente in caso di necessità dovuto alla flagranza dell'illecito commesso nel territorio di appartenenza. Diversamente, fuori da tale ipotesi, l'attività di polizia giudiziaria della Polizia locale è consentita esclusivamente "alla dipendenza e sotto la direzione dell'autorità giudiziaria" (art. 56 c.p.p.), limitatamente agli "atti ad essa specificamente delegati a norma dell'articolo 370, esegue[ndo] le direttive del pubblico ministero", essendo invece preclusa ogni attività di iniziativa propria.

Per quanto concerne, invece, le funzioni di pubblica sicurezza della polizia locale, l'art. 5, comma 1, lett. c), della l. 7 marzo 1986, n. 65 prevede che "il personale che svolge servizio di polizia municipale, nell'ambito territoriale dell'ente di appartenenza e nei limiti delle proprie attribuzioni, esercita anche […] funzioni ausiliarie di pubblica sicurezza"; ciò "collaboran[d]o, nell'ambito delle proprie attribuzioni, con le Forze di polizia dello Stato, previa disposizione del sindaco, quando ne venga fatta, per specifiche operazioni, motivata richiesta dalle competenti autorità" (art. 3). A tal fine, il Prefetto conferisce al personale delle Polizia locale, previa comunicazione del Sindaco, la qualità di agente di pubblica sicurezza, dopo aver accertato il possesso dei requisiti previsti dalla legge (art. 5, comma 2). Nell'esercizio delle funzioni di agente di pubblica sicurezza, tale personale, messo a disposizione dal Sindaco, dipende operativamente dalla competente autorità di pubblica sicurezza nel rispetto di eventuali intese fra dette autorità e il Sindaco (art. 5, comma 4).

Nel caso di specie - in cui comunque non risulta che il Comune sia venuto a conoscenza dei dati personali relativi ai presunti autori dei reati segnalati, ovvero n. 19 casi di furto -, l'Ente non ha comprovato che la raccolta delle segnalazioni dei cittadini, finalizzata alla pianificazione delle attività di pubblica sicurezza del territorio, sia stata effettuata su richiesta delle competenti autorità di pubblica sicurezza.

Pertanto, non avendo la Polizia locale del Comune una competenza generale in materia, deve ritenersi che il trattamento dei dati personali in questione sia stato effettuato in maniera non conforme al principio di "liceità, correttezza e trasparenza" e in assenza di una base giuridica, in violazione degli artt. 5, par. 1, lett. a) e 6 del Regolamento, nonché 2-ter del Codice.

3.2.2 L'errata qualificazione dei ruoli in materia di protezione dei dati personali e la mancata stipula di un accordo sulla protezione dei dati con il responsabile del trattamento

Ai sensi dell'art. 28, par. 3, del Regolamento, "i trattamenti da parte di un responsabile del trattamento devono essere disciplinati da un contratto o da altro atto giuridico a norma del 26 diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento, che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento", e che preveda tutti gli impegni previsti dal medesimo art. 28, par. 3, del Regolamento (cfr. cons. 81 del Regolamento).

Il contratto o il diverso atto giuridico devono essere "stipulat[i] in forma scritta, anche in formato elettronico" (art. 28, par. 9, del Regolamento).

Nel corso dell'istruttoria è emerso che il Comune ha assunto il ruolo di responsabile del trattamento nel rapporto con la Società, fornitrice dell'applicazione "TrevisoSicura", qualificatasi come titolare del trattamento dei dati personali degli utenti di tale applicazione.

Come riconosciuto dal Comune, l'Ente avrebbe, invece, dovuto qualificarsi come titolare del trattamento, in quanto soggetto a cui sono riconducibili le finalità e i mezzi del trattamento e che ha determinato gli stessi. Per converso, il fornitore dell'applicazione avrebbe dovuto essere qualificato come responsabile del trattamento, avendo lo stesso trattato i predetti dati personali non già per proprie finalità, bensì per conto e nell'interesse del Comune.

Ciò premesso, deve rilevarsi che il Comune, in quanto titolare del trattamento, ha omesso di stipulare un accordo sulla protezione dei dati personali con il predetto fornitore, quale responsabile del trattamento.

Al riguardo, deve evidenziarsi che, come chiarito dal Comitato europeo per la protezione dei dati, "poiché il regolamento stabilisce con chiarezza l'obbligo di stipulare un contratto scritto, qualora non sia in vigore nessun altro atto giuridico pertinente si ha una violazione del [Regolamento], ovvero dell'"articolo 28, paragrafo 9, del [Regolamento]". Considerato che "sia il titolare sia il responsabile del trattamento hanno la responsabilità di garantire l'esistenza di un contratto o di un altro atto giuridico che disciplini il trattamento", l'autorità di controllo compente "potrà infliggere una sanzione amministrativa pecuniaria sia al titolare sia al responsabile del trattamento" ("Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR", adottate dal Comitato europeo per la protezione dei dati il 7 luglio 2021, par. 103).

Pertanto, laddove, come nel caso di specie, sussista "un rapporto titolare-responsabile del trattamento […] anche in assenza di un [valido] accordo di trattamento per iscritto" - in quanto il soggetto che tratta i dati effettua in concreto il trattamento non per proprie finalità ma per conto del soggetto committente e titolare del trattamento, nell'esecuzione di un contratto di servizi o di altro analogo rapporto giuridico in essere tra le parti (cfr. la definizione di "responsabile del trattamento" di cui all'art. 4, par. 1, n. 8, del Regolamento) - "ciò implic[a] […] una violazione dell'articolo 28, paragrafo 3, del [Regolamento]" (ibidem, par. 103 e nota n. 42).

Atteso che, nel caso di specie, non è stato stipulato un accordo sulla protezione dei dati personali con il fornitore e manutentore dell'applicazione informatica "TrevisoSicura", che ha agito in concreto quale responsabile del trattamento, deve concludersi che il Comune ha posto in essere una violazione dell'art. 28, par. 3, del Regolamento.

3.2.3 L'inidonea informativa sul trattamento dei dati personali

Anche in ragione della scorretta qualificazione dei ruoli in materia di protezione dei dati personali, l'informativa sul trattamento dei dati personali che è stata resa agli utenti dell'applicazione "TrevisoSicura" (in atti), non può ritenersi pienamente conforme ai requisiti previsti dall'art. 13 del Regolamento.

Ciò in quanto tale informativa:

- indica erroneamente la Società quale titolare del trattamento in luogo del Comune, di cui non sono indicati i dati di contatto (v. art. 13, par. 1, lett. a), del Regolamento);

- non indica i dati di contatto del Responsabile della protezione dei dati designato dal Comune (v. art. 13, par. 1, lett. b), del Regolamento);

- omette di far riferimento, quale base giuridica del trattamento, alla necessità di esercitare compiti di interesse pubblico propri del Comune (v. art. 13, par. 1, lett. c), del Regolamento);

- non cita la Società tra i destinatari dei dati nella veste di responsabile del trattamento (v. art. 13, par. 1, lett. e), del Regolamento);

- indica un tempo di conservazione dei dati ("al massimo 12 mesi") che non corrisponde a quello indicato nella pagina web dell'applicazione ("3 mesi dalla segnalazione con successiva cancellazione automatica") (v. art. 13, par. 2, lett. a), del Regolamento);

- non menziona il diritto dell'interessato di proporre reclamo a un'autorità di controllo (v. art. 13, par. 2,

lett. d), del Regolamento);

- non chiarisce se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze del mancato conferimento degli stessi (v. art. 13, par. 2, lett. e), del Regolamento).

Deve, pertanto, concludersi che il Comune, in veste di titolare del trattamento, su cui gravano gli obblighi in materia di trasparenza previsti dalla normativa in materia di protezione dei dati, ha agito in violazione degli artt. 5, par. 1, lett. a), e 13 del Regolamento.

3.2.4 La violazione dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita, nonché di responsabilizzazione

Dalla complessiva istruttoria avviata nei confronti del Comune è emerso che l'Ente ha messo a disposizione degli utenti l'applicazione informatica "TrevisoSicura", senza aver, tuttavia, adottato alcun atto interno volto a disciplinare il trattamento e ad assicurare il complessivo rispetto della normativa in materia di protezione dei dati, essendosi, peraltro, erroneamente attribuito il ruolo di responsabile del trattamento (v. le citate dichiarazioni del Comune in merito alla circostanza che "al momento non sono stat[e] adottate determinazioni volte a disciplinare i trattamenti di dati personali derivanti dalla messa a disposizione della app dovute all'errata identificazione dei ruoli previsti dal Regolamento. Le uniche determinazioni riguardano l'attivazione/manutenzione del servizio per gli anni 2021 e 2022").

L'Ente non ha, pertanto, individuato, prima di iniziare il trattamento e fin dalla progettazione dell'applicazione, le necessarie misure volte ad attuare i principi di protezione dei dati, integrando nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento (v. art. 25, par. 1, del Regolamento).

Né, sono state messe in atto misure tecniche e organizzative adeguate al fine di garantire che venissero trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (v. art. 25, par. 2, del Regolamento). In particolare, il Comune, configurando l'applicazione in maniera tale da concedere agli interessati la possibilità di inserire del testo libero in uno specifico campo, non ha considerato la possibilità che gli stessi potessero inviare all'Ente dati non pertinenti rispetto alla finalità perseguita (cfr. art. 5, par. 1, lett. c), che formalizza il principio di "minimizzazione dei dati"), ovvero la mappatura delle zone della città interessata da fenomeni criminali, con il conseguente rischio di acquisire dati appartenenti a categorie particolari (cfr. art. 9 del Regolamento) o a reati (cfr. art. 10 del Regolamento).

Il Comune ha poi dichiarato che "al momento il periodo di conservazione delle segnalazioni riportato nell'informativa è al massimo 12 mesi", mentre "nella pagina web della app è invece riportato un tempo di conservazione di 3 mesi dalla segnalazione con successiva cancellazione automatica". Fermo restando che sussiste un'incongruenza con riguardo ai tempi di conservazione dichiarati nell'informativa e quelli menzionati nella pagina web dell'applicazione, il Comune ha comunque riconosciuto che "in considerazione della finalità e soprattutto della modalità di routing delle segnalazioni, si ritiene, al fine di ridurre considerevolmente la superficie di esposizione e conseguentemente i rischi per gli interessati, di evitare a monte tale conservazione da parte dei sistemi o comunque di limitare ad un numero di giorni compatibili con eventuali problematiche di ricezione della posta elettronica, aggiornando conseguentemente l'informativa". Pertanto, come ammesso dallo stesso Comune, la conservazione delle segnalazioni nei sistemi informatici del fornitore, dopo l'invio delle stesse alla Polizia locale a mezzo posta elettronica, non era, in ogni caso, necessaria.

Dalle considerazioni che precedono emerge che il Comune non è stato in grado di comprovar di aver rispettato i principi di protezione dei dati e di aver tenuto in debito conto i profili di protezione dei dati personali prima di mettere l'applicazione "TrevisoSicura" a disposizione degli utenti, venendo, così, meno agli obblighi derivanti dal principio di responsabilizzazione, che informa la disciplina europea in materia di protezione dei dati (v. artt. 5, par. 2, e 24, parr. 1 e 2, del Regolamento).

Deve, pertanto, concludersi che il Comune ha agito in maniera non conforme ai principi di responsabilizzazione e protezione dei dati fin dalla progettazione e per impostazione predefinita, in violazione degli artt. 5, par. 2 (in combinato disposto con l'art. 24), e 25 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 nel contesto dell'utilizzo dell'applicazione "TrevisoSicura", in violazione degli artt. 5, par. 1, lett. a) e par. 2 (in combinato disposto con l'art. 24), 6, 13, 25 e 28, par. 3, 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 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 le funzionalità di segnalazione dell'applicazione informatica sono state disattivate e che risulta trascorso il periodo massimo di conservazione delle segnalazioni già ricevute, 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).

La violazione delle disposizioni citate è soggetta all'applicazione di una sanzione amministrativa pecuniaria ai sensi del combinato disposto di cui agli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento.

La 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:

- sebbene l'applicazione informatica "TrevisoSicura" sia stata messa a disposizione degli utenti per un esteso arco temporale (dal mese di luglio 2020 al mese di dicembre 2022), il Comune ha ricevuto un numero non elevato di segnalazioni (n. 414) e, pertanto, il trattamento ha riguardato un numero limitato di interessati rispetto al numero totale dei residenti nel Comune (circa 85.000 abitanti) (cfr. art. 83, par. 2, lett. a), del Regolamento);

- il rapporto tra il Comune e la Società, oltre a non essere stato definitivo in un accordo sulla protezione dei dati stipulato ai sensi dell'art. 28, par. 3, del Regolamento, non è stato correttamente inquadrato, per i profili di protezione dei dati, nemmeno nell'ambito del contratto di fornitura dei servizi di manutenzione (v. l'email della Società del 5 maggio 2023, acquisita nell'ambito del separato ma connesso procedimento avviato nei confronti della stessa, ove si afferma che il rapporto di committenza tra il Comune e la Società "non trova alcuna regolazione se non in uno scarno disciplinare" (cfr. art. 83, par. 2, lett. a), del Regolamento);

- la violazione ha carattere colposo (cfr. art. 83, par. 2, lett. b), del Regolamento);

- il trattamento non ha riguardato dati personali appartenenti a categorie particolari (v. art. 9 del Regolamento) o dati relativi a reati (v. art. 10 del Regolamento), sebbene, come sopra illustrato, la circostanza che l'applicazione sia stata configurata in maniera tale da consentire agli utenti

l'inserimento di testo libero ha esposto il Comune al rischio di acquisire anche tali tipologie dati (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, si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze attenuanti:

- il Comune ha un alto grado di responsabilità, avendo sostanzialmente omesso di considerare i profili di protezione dei dati sottesi al trattamento in questione, prima di effettuare lo stesso (art. 83, par. 2, lett. d), del Regolamento);

- il Comune ha offerto una buona cooperazione con l'Autorità nel corso dell'istruttoria, essendosi, altresì, prontamente attivato al fine di disattivare le funzionalità di segnalazione dell'applicazione informatica subito dopo aver appreso dell'avvio dell'istruttoria (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 7.000 (settemila) per la violazione degli artt. 5, par. 1, lett. a) e par. 2 (in combinato disposto con l'art. 24), 6, 13, 25 e 28 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.

Tenuto conto che il trattamento dei dati personali in questione ha avuto luogo in violazione delle predette disposizioni del Regolamento per un esteso arco temporale e che, come è emerso dell'istruttoria, il Comune ha sostanzialmente omesso di considerare i profili di protezione dei dati prima di porre l'applicazione a disposizione degli utenti, si ritiene, altresì, che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7 del Codice e art. 16 del Regolamento del Garante n. 1/2019.

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

TUTTO CIÒ PREMESSO IL GARANTE

dichiara, ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, l'illiceità del trattamento effettuato dal Comune di Treviso per violazione degli artt. 5, par. 1, lett. a) e par. 2 (in combinato disposto con l'art. 24), 6, 13, 25 e 28 del Regolamento, nonché 2-ter del Codice, nei termini di cui in motivazione;

ORDINA

al Comune di Treviso, in persona del legale rappresentante pro-tempore, con sede legale in Via Del Municipio, 16 - 31100 Treviso (TV), C.F. 80007310263, di pagare la somma di euro 7.000 (settemila) 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 7.000 (settemila) 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

- l'archiviazione, ai sensi dell'art. 14 del Regolamento del Garante n. 1/2019, della contestazione riguardante il trattamento dei dati personali effettuato mediante l'impiego dei droni dotati di telecamere termiche da parte della Polizia locale;

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

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

Ai sensi degli artt. 78 del Regolamento, 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento è possibile proporre ricorso dinnanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 4 luglio 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Mattei