



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Provvedimento del 23 settembre 2026 [10304881]

[doc. web n. 10304881]

Provvedimento del 23 settembre 2026

Registro dei provvedimenti
n. 636 del 23 settembre 2026

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzone, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia, componente, 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 Stanzone;

PREMESSO

1. Introduzione.

Con reclamo presentato ai sensi degli artt. 77 del Regolamento nei confronti del Comune di Arvier, la Sig.ra XX, per il tramite del proprio avvocato, ha lamentato la circostanza che il Comune avrebbe installato una telecamera di videosorveglianza sulla pubblica via, con angolo di visuale impostato in maniera tale da riprendere anche la propria privata abitazione.

2. L’attività istruttoria.

In riscontro a una richiesta d’informazioni (v. nota prot. n. XX del XX), formulata ai sensi dell’art. 157 del Codice, il Comune, con nota prot. n. XX del XX, ha dichiarato, in particolare, che:

- “il sistema comunale di videosorveglianza [...] come risulta dalle deliberazioni della Giunta comunale n. 37/2011 [...] e n. 43/2012 [...] trova fondamento nelle attribuzioni riconosciute ai Comuni dall’art. 13 del D.Lgs. 267/2000 (TUEL), nonché negli artt. 50 e 107 del medesimo decreto, in relazione alle funzioni di amministrazione e gestione del territorio. La relativa base giuridica è individuata nell’art. 6, par. 1, lett. e) del Regolamento [...]”;
- “l’impianto originario è stato realizzato negli anni 2011-2012 nell’ambito del contributo regionale concesso con DGR n. 707/2011, in attuazione dell’art. 11-bis della L.R. Valle d’Aosta n. 11/2005”;
- “la disciplina è stata attuata con d.g.r. n. 707/2011 [...], che individuava in modo specifico requisiti degli impianti, caratteristiche, modalità di valutazione dei progetti oggetto di realizzazione e finanziamento [...], modalità di realizzazione e successiva gestione degli impianti”;
- “tale disciplina regionale è antecedente al D.L. 20 febbraio 2017, n. 14, che ha introdotto, nel resto del territorio nazionale, il meccanismo dei “patti per l’attuazione della sicurezza urbana” con le Prefetture [...], fermo restando che] le funzioni prefettizie nel territorio valdostano sono esercitate dalla Regione stessa”;
- “nel caso di specie, l’impianto di videosorveglianza è stato approvato e finanziato dalla Regione Valle d’Aosta nell’ambito della disciplina regionale vigente all’epoca”;
- “dagli allegati alla domanda di finanziamento [...] emergono le finalità dello stesso [...], ossia “prevenzione dei fenomeni di inciviltà urbana e di criminalità al fine di garantire l’incolumità delle persone negli edifici pubblici, nelle scuole, nei parchi, nelle aree verdi, nei parcheggi ed in altre aree comunali a rischio; controllo dell’ambiente, del territorio e delle aree sensibili; controllo della viabilità pubblica; tutela del patrimonio pubblico”;
- “tali finalità hanno determinato le scelte sul posizionamento delle telecamere, che riprendevano i principali assi viari regionali anche a fini di protezione civile, gli accessi ai parcheggi comunali e l’accesso al borgo centrale del Comune [...]”;
- “l’intervento è stato oggetto di un successivo ampliamento, realizzato nel 2013, per l’installazione di n. 5 telecamere destinate esclusivamente alla lettura delle targhe nei parcheggi già oggetto di videosorveglianza, e di un ulteriore ampliamento negli anni 2015–2016 [...]”;
- “tale intervento risulta riconducibile a esigenze di organizzazione della circolazione urbana nel principale snodo di accesso al paese e alle scuole comunale, di gestione dell’unica area di sosta rimasta priva di copertura video e di tutela del patrimonio comunale, essendo in quella sede posizionati alcune postazioni della raccolta rifiuti: si tratta di finalità strettamente amministrative rientranti nelle competenze ordinarie dell’Ente locale. L’ampliamento, intervenuto anch’esso anteriormente al D.L. n. 14/2017, non si è configurato come iniziativa finalizzata alla sicurezza urbana in senso stretto”;
- “[...] la videocamera oggetto di [reclamo...] è stata posizionata con esclusivo riferimento al controllo del parcheggio comunale antistante e della limitrofa area per conferimento rifiuti, nonché per la regolazione della viabilità sulla via pubblica antistante, che conduce al nuovo edificio scolastico [...]”;
- con l’”ampliamento del 2015” sono state installate “due telecamere a specchio che riprendono: l’una [...] la strada di accesso alla Biblioteca (nuovo plesso scolastico) e il parcheggio situato ad est di questo edificio [...]; l’altra [...] che permette di sorvegliare la rotonda e il parcheggio pubblico antistante il fabbricato delle ex scuole, l’area davanti al quale è adibita a parcheggio”;
- “il posizionamento prescelto per la telecamera [...] era [...] dettato da due necessità tecniche: posizionare la telecamera in corrispondenza del ripetitore, onde evitare un collegamento aggiuntivo, e individuare un angolo visuale in grado di rispondere alla doppia esigenza di “coprire” sia l’area di parcheggio nella sua interezza [...] sia l’incrocio antistante”;
- “[...] il raggio della telecamera intercetta la facciata esterna dell’immobile della reclamante, in ragione del posizionamento della stessa a confine con l’area pubblica adibita a parcheggio e del fronte stante edificio delle ex scuole”;

- “la distanza della telecamera dall’oggetto della ripresa (il parcheggio) e la necessità di coprirne tutto il fronte e l’incrocio hanno determinato l’angolo di campo prescelto, condizionato anche dal fatto che le telecamere sono posizionate al coperto, nella torretta sovrastante l’edificio in corrispondenza come detto del ripetitore, e quindi con limitata capacità di angolare la ripresa diversamente, senza riprendere anche altre abitazioni [...]”;
- “la telecamera era comunque posizionata in modo tale da non riprendere in alcun modo l’accesso alla abitazione privata (che è situato molto più a ovest [...]) e non era in grado di riprendere ambienti interni o spazi riservati [...]”;
- “a seguito del reclamo e di un audit tecnico condotto con il coinvolgimento del DPO, in data XX [...] è stato attivato un sistema di privacy masking digitale permanente sulla porzione di immobile interessata. Tale tecnologia garantisce l’oscuramento automatico e irreversibile dell’area privata [...]”;
- “l’impianto, nella sua conformazione originaria, risultava segnalato da n. 4 cartelli informativi di primo livello [...]. Si tratta dei cartelli oggi rimossi per lavori e altre esigenze e o rimossi in data XX [...]”;
- “a seguito della segnalazione del Garante si è proceduto all’ampliamento e all’aggiornamento della rete cartellonistica, provvedendo all’installazione di pannelli provvisori nei punti indicati dalla mappa. La sostituzione è avvenuta nella giornata del XX [...] Nel frattempo sono state avviate le procedure amministrative per la fornitura della cartellonistica definitiva”;
- “risultano, quindi, ad oggi installati 20 cartelli, di cui due nell’area oggetto della segnalazione in parola, all’altezza di via Lostan, e uno in corrispondenza delle scuole [...]”;
- “l’informativa di secondo livello è consultabile sul sito comunale all’indirizzo <https://arvier.eu/privacy/informativa-privacy-videosorveglianza/>”, nel testo “disponibile sino al 2022 [...e in quello] redatto successivamente alla presa di funzione del nuovo DPO”;
- “le informative sono ed erano disponibili on line e accessibili nella apposita sezione del sito internet comunale dall’installazione dell’impianto di videosorveglianza. In ragione delle verifiche operate successivamente al ricevimento della nota [del] Garante si è rilevato un malfunzionamento del link in questione, che è stato prontamente ripristinato in data XX”;
- “risulta [...] documentabile che l’informativa specifica relativa alla videosorveglianza sia stata caricata sul sito nel novembre 2022 e sia rimasta consultabile sino - perlomeno - al 20 giugno 2024, coprendosi così integralmente il periodo di tempo in cui viene contestata la ripresa abusiva, che risale all’11 maggio 2023”;
- “il Comune [...] ha adottato valutazione di impatto in data 30 luglio 2018, quando l’impianto si presentava già nella sua conformazione attuale. Il documento sarà stato oggetto di prossimo aggiornamento, per attualizzarlo all’evoluzione normativa [...]”.

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 degli interessati per finalità amministrative, senza aver individuato per ciascuna di esse una chiara base giuridica, dotata dei necessari requisiti di rango e qualità, avendo l’Ente agito in maniera non conforme al principio di “liceità, correttezza e trasparenza” e in assenza di base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6, par. 1, lett. c) ed e), e parr. 2 e 3, del Regolamento, nonché 2-ter del Codice; per aver sottoposto a videosorveglianza la privata abitazione della reclamante, in contrasto con i principi di “minimizzazione dei dati” e “protezione dei dati fin dalla progettazione e protezione per impostazione predefinita”, con conseguente violazione degli artt. 5, par. 1, lett. c) e 25 del Regolamento; per non aver assicurato la necessaria trasparenza del trattamento nei confronti degli interessati, in contrasto con il principio di “liceità, corretta e trasparenza” e in violazione degli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento; per non aver svolto una valutazione di impatto sulla protezione dei dati entro la data in cui il Regolamento è diventato efficace (25 maggio 2018), 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, le cui parti essenziali sono riprese nella parte motiva del presente provvedimento.

3. Esito dell'attività istruttoria.

3.1 La liceità del trattamento.

Al fine di garantire un elevato livello di protezione delle libertà e dei diritti fondamentali delle persone fisiche, in particolare del loro diritto al rispetto della vita privata e alla protezione dei dati personali, sancito dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (cfr. art. 1 del Regolamento), qualsiasi trattamento di dati personali deve essere conforme ai principi enunciati all'art. 5 del Regolamento - inclusi 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) - e deve soddisfare le condizioni di liceità di cui all'art. 6 del Regolamento.

In tale quadro, i soggetti pubblici possono, di regola, trattare dati personali, anche mediante dispositivi video, se il trattamento è necessario "per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" o "per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" (art. 6, par. 1, lett. c) ed e), del Regolamento; 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).

Gli Stati membri "possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del [...] regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto [...]" (art. 6, par. 2, del Regolamento).

La base su cui si fonda il trattamento dei dati di cui all'art. 6, par. 1, lett. c) ed e), del Regolamento, stabilita dal diritto dell'Unione o dal diritto dello Stato membro, deve soddisfare un sufficiente livello di qualità, disciplinando gli elementi essenziali del trattamento (v. art. 6, par. 3, del Regolamento; cfr. cons. 45 del Regolamento); in conformità alla giurisprudenza della Corte di giustizia dell'Unione europea e a quella della Corte europea dei diritti dell'uomo, essa deve essere, infatti, chiara e precisa e prevedibile per gli interessati (v. cons. 41 del Regolamento).

In attuazione delle predette disposizioni del Regolamento, il legislatore nazionale ha previsto che "la base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento è costituita da una norma di legge o di regolamento o da atti amministrativi generali" (art. 2-ter, comma 1, del Codice).

Nel caso di specie, il Comune, a partire dal 2011/2012, ha attivato un sistema di videosorveglianza sul proprio territorio, con un ampliamento dello stesso prima nel 2013 (con l'attivazione di cinque telecamere per la lettura delle targhe in aree di parcheggio) e poi nel 2015/2016 (estensione del controllo dei parcheggi comunali e di alcuni tratti della viabilità urbana, tramite due nuove telecamere; implementazione di sistemi di lettura targhe connessi alla gestione della sosta; potenziamento dell'infrastruttura tecnica).

Per quanto concerne i presupposti di liceità del trattamento, il Comune, oltre ad aver fatto riferimento alla finalità di tutela della sicurezza urbana - rispetto alla quale, anche tenuto conto delle peculiarità proprie dell'ordinamento della Regione Autonoma Valle d'Aosta, non sono state mosse contestazioni nel corso del procedimento - ha affermato che "il sistema comunale di videosorveglianza si inserisce nell'ambito delle funzioni amministrative proprie dell'Ente locale", menzionando una pluralità di finalità di trattamento, caratterizzate, tuttavia, da genericità ed eterogeneità (gestione del territorio; tutela del patrimonio comunale; controllo della viabilità urbana; tutela ambientale; protezione civile; controllo delle aree di parcheggio; ecc.).

In relazione a dette finalità, la base giuridica del trattamento sarebbe da rinvenirsi, ad avviso del Comune, negli artt. 13, 50 e 107 del d.lgs. 18 agosto 2000, n. 267 (Testo unico delle leggi sull'ordinamento degli enti

locali – TUEL), disposizioni che, tuttavia, si limitano ad attribuire agli enti locali le funzioni amministrative che riguardano la popolazione ed il territorio comunale, nonché a disciplinare le competenze del Sindaco e le funzioni e responsabilità della dirigenza, ma che non regolano in alcun modo l'impiego di dispositivi video a fini amministrativi e i connessi trattamenti di dati personali, non soddisfacendo, pertanto, le stesse, i requisiti di qualità della base giuridica richiesti dalla quadro giuridico in materia di protezione dei dati.

Anche l'art. 11-bis della legge regionale n. 11/2005, invocato in sede di memoria difensiva, si limita a prevedere che, “al fine di garantire migliori condizioni di sicurezza, ai sensi degli articoli 1, comma 2, lettera d), e 2, la Regione promuove e sostiene progetti volti a favorire un sistema integrato di sicurezza sul territorio, mediante la concessione agli enti locali di contributi per la realizzazione di progetti di investimento in tecnologie per la sicurezza del territorio, nel rispetto della normativa vigente in materia di protezione dei dati personali”. Tale disposizione, che riguarda il diverso ambito della sicurezza integrata (cfr. art. 1, comma 2, del d.l. 20 febbraio 2017, n. 14), attiene unicamente allo stanziamento di fondi per la realizzazione, a livello locale, di “progetti di investimento in tecnologie per la sicurezza del territorio”, ma non disciplina gli elementi essenziali del trattamento, non potendo, pertanto, costituire, per difetto dei necessari requisiti di qualità, la base giuridica del trattamento.

Né rileva, come sostenuto sempre in sede di memoria difensiva, che, in esecuzione di tale disposizione della legge regionale, che la DGR n. 707/2011 specifichi che la nozione di “sistema integrato di sicurezza sul territorio” debba essere intesa “non solamente come attività di pubblica sicurezza, ma anche come attività tesa a garantire il controllo dell'ambiente, del territorio e delle aree sensibili”, ricomprendendo la stessa, oltre alla “prevenzione dei fenomeni di inciviltà urbana e di criminalità” anche il “controllo dell'ambiente, del territorio e delle aree sensibili”, il “controllo della pubblica viabilità” e la “tutela del patrimonio pubblico”, essendo, in tale quadro, “maggiormente valutati i progetti che [...] permettono di rilevare dati sugli assi viari statali e regionali, di interesse sia per le Forze di Polizia, sia per la protezione civile, anche a completamento degli impianti di videosorveglianza già esistenti”. In disparte, in questa sede, da ogni considerazione in merito alla possibilità di ampliare, con una delibera di giunta regionale, la nozione di sicurezza integrata definita dalla legge nazionale e regionale, deve, in ogni caso, osservarsi che anche tale delibera disciplina soltanto il finanziamento di progetti realizzati in tale ambito, ma non costituisce essa stessa la base giuridica dei trattamenti di dati personali posti in essere dai Comuni, per finalità amministrative, mediante i dispositivi video oggetto di finanziamento.

D'altra parte, l'impiego di dispositivi elettronici, anche video, per finalità amministrative riconducibili all'ambito della tutela ambientale e a quello della circolazione e sicurezza stradale, è già disciplinato dal legislatore nazionale in maniera uniforme per tutto il territorio italiano (v., in particolare, il d.lgs. 30 aprile 1992, n. 285 - “Nuovo codice della strada”, e il d.lgs. 3 aprile 2006, n. 152 - “Norme in materia ambientale”), stante la potestà legislativa esclusiva dello Stato tanto nella materia dell’“ordine pubblico e sicurezza, ad esclusione della polizia amministrativa locale” (art. 117, comma 2, lett. h), Cost.; cfr. Cort. Cost., sent. n. 69 del 2023, ove si evidenzia che la Corte “ha già ricondotto la disciplina della circolazione stradale alla competenza legislativa esclusiva dello Stato in tema di ordine pubblico e sicurezza, in quanto volta a prevenire la commissione di reati incidenti sulla incolumità personale (sentenza n. 428 del 2004; ex multis, sentenze n. 129 del 2021, n. 77 del 2013 e n. 223 del 2010)” quanto nella materia della “tutela dell'ambiente” (art. 117, comma 2, lett. s), Cost., fermo restando quanto previsto dall'art. 3-quinques, comma 2, del d.lgs. 3 aprile 2006, n. 152, ai sensi del quale “le regioni e le province autonome di Trento e di Bolzano possono adottare forme di tutela giuridica dell'ambiente più restrittive, qualora lo richiedano situazioni particolari del loro territorio, purché ciò non comporti un'arbitraria discriminazione, anche attraverso ingiustificati aggravati procedurali”; cfr. Cort. cost., sent. nn. 70/2011, 373/2010, 341/2010 e 307/2003).

Il medesimo limite trova applicazione anche con riferimento al “Regolamento [comunale] per la disciplina della videosorveglianza”, che, come sostenuto nelle memorie difensive, costituirebbe “atto amministrativo generale ai sensi dell'art. 2-ter, comma 1, del Codice Privacy [...] disciplina puntualmente tutti gli elementi essenziali del trattamento [, tra cui] le finalità (art. 4, comma 2: prevenzione e tutela della pubblica sicurezza e ambientale; ricostruzione dinamica di atti vandalici; vigilanza sul pubblico traffico; protezione civile sul territorio urbano)”. Tralasciando, in questa sede, ogni considerazione in merito alla riconducibilità di siffatto regolamento comunale alla categoria giuridica dell'atto amministrativo generale, deve, infatti, osservarsi che, come già chiarito dall'Autorità, un trattamento di dati personali in ambito pubblico non può comunque trovare fondamento nelle disposizioni di un atto amministrativo generale, poiché esse non possono contravvenire o modificare le norme sovraordinate di riferimento, potendo, invece, soltanto integrare

l'ordinamento nel sistema della gerarchia delle fonti di diritto interno. Ciò in quanto non sono consentiti livelli differenziati di tutela della protezione dei dati personali, né su base territoriale né a livello di singola amministrazione, specie quando la materia sia già stata oggetto di bilanciamento e di uniforme trattamento da parte del legislatore a livello nazionale, perlopiù, come in questo caso, in forza di una potestà legislativa esclusiva (v. provv. 11 aprile 2024, n. 235, doc. web n. 10019523; v. anche Newsletter del 6 giugno 2024, doc. web n. 10022928). Pertanto, il regolamento in questione, adottato dal Comune anche ai sensi dell'art. 3 della DGR n. 707/2011, ai sensi del quale “le modalità operative di utilizzo degli impianti di videosorveglianza devono essere disciplinate da apposito regolamento dell'ente, da adottarsi in conformità alla normativa statale vigente in materia di protezione dei dati personali, nonché ai provvedimenti del Garante per la protezione dei dati personali in materia di videosorveglianza”, avrebbe potuto contenere la disciplina di dettaglio del trattamento, in considerazione delle specificità tecniche e organizzative proprie dell'Ente, ma non anche introdurre trattamenti non previsti dalle sovraordinate disposizioni di legge di riferimento in materia.

Dette considerazioni valgono anche per la specifica telecamera oggetto di reclamo, che sarebbe funzionale al “controllo del parcheggio comunale [...] e la regolazione della viabilità pubblica nella zona”.

Tali generiche finalità di controllo della viabilità, - intesa come possibilità di avere contezza dei volumi complessivi di traffico e di eventuali blocchi dello stesso - possono, peraltro, essere perseguite utilizzando dispositivi video che non comportano un trattamento di dati personali, ad esempio in ragione del fatto che il loro livello di risoluzione è sufficientemente basso da non consentire il riconoscimento delle persone fisiche riprese o la lettura dei numeri di targa dei veicoli in transito (v. il già citato provvedimento generale del Garante in materia di videosorveglianza del 2010, ove si rammenta di “non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (es., configurando il [sistema] in modo da consentire, per monitorare il traffico, solo riprese generali che escludano la possibilità di ingrandire le immagini e rendere identificabili le persone)”).

Nel presentare la propria memoria, il Comune, quanto alla circostanza che “nella prima risposta istruttoria, ha qualificato le finalità della telecamera [oggetto di reclamo] come “esclusivamente amministrative”, ha sostenuto, mutando in parte la propria tesi difensiva, che “[detta] telecamera persegue finalità che si inscrivono propriamente nel concetto di sicurezza integrata, distinto tanto dalla sicurezza urbana in senso stretto (prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria ex art. 4 d.l. 14/2017) quanto da mere finalità burocratico-amministrative”. In particolare, “il controllo del parcheggio comunale antistante e della viabilità di accesso al plesso scolastico risponde a esigenze di sicurezza della circolazione e di tutela degli utenti deboli (bambini, pedoni)” e “il monitoraggio dell'area di conferimento rifiuti (isola ecologica) costituisce esercizio del potere-dovere di tutela del patrimonio pubblico, nella specie del patrimonio indisponibile del Comune”. Ad avviso del Comune, “queste finalità, lette unitariamente, configurano un sistema di sicurezza integrata del territorio comunale: non si tratta di mero controllo amministrativo fine a sé stesso, né di sicurezza urbana in senso stretto (che richiederebbe il patto con la Prefettura), bensì di un presidio tecnologicamente avanzato che coniuga sicurezza stradale, tutela del patrimonio pubblico e protezione civile, esattamente nella logica della sicurezza integrata descritta dall'art. 1 del d.l. 14/2017”. Tale affermazione conferma le difficoltà dell'Ente a rinvenire la corretta base giuridica di ciascun trattamento posto in essere mediante i dispositivi di videosorveglianza installati sul proprio territorio. Deve, infatti, osservarsi che l'art. 2 del d.l. 20 febbraio 2017, n. 14 rimette a specifiche “Linee generali per la promozione della sicurezza integrata”, da adottarsi su proposta del Ministro dell'interno, con accordo sancito in sede di Conferenza Unificata, la definizione delle aree di collaborazione tra le forze di polizia e la polizia locale, in alcuni specifici settori di intervento, tra i quali, per quanto in questa sede d'interesse, “l'utilizzo in comune di sistemi di sicurezza tecnologica finalizzati al controllo delle aree e delle attività soggette a rischio”. Dette Linee generali, adottate in sede di Conferenza Unificata in data 24 gennaio 2018, fanno esclusivo riferimento, quanto a tali “sistemi di sicurezza tecnologica”, ai sistemi di videosorveglianza, precisando che “l'utilizzazione in comune dei sistemi dovrà avvenire in ossequio al principio del “rispetto delle rispettive competenze” [...] e a quelli di “pertinenza e non eccedenza” dei trattamenti dei dati personali rispetto ai compiti istituzionali assegnati, sanciti dal ricordato “Codice della privacy””. Ciò con la conseguenza che le invocate disposizioni del d.l. 20 febbraio 2017, n. 14 in materia di sicurezza integrata riguardano esclusivamente il possibile impiego in comune, da parte di forze di polizia e polizia locale, dei rispettivi sistemi di videosorveglianza, ma non costituiscono esse stesse la base giuridica dei trattamenti posti in essere a monte dai Comuni per le finalità amministrative o di sicurezza urbana di propria competenza, che, invece,

rinvengono la propria legittimazione nella disciplina di settore che attribuisce loro dette competenze e che disciplina in dettaglio i trattamenti di dati eseguibili.

In merito alla circostanza che la telecamera oggetto di reclamo fosse preordinata al “monitoraggio dell’area di conferimento rifiuti (isola ecologica)”, meglio prospettata in sede di memoria difensiva, si rileva una sostanziale ambiguità della posizione assunta dall’Ente, che in un successivo passaggio di tale memoria difensiva ha affermato che “tale ultimo aspetto [, relativo all’isola ecologica,] si sovrappone a quello del controllo dell’ambiente”. Risulta, comunque, assorbente il fatto che, come emerge chiaramente dalla documentazione in atti (v. all. 20-bis alla nota del Comune del XX), detta telecamera riprende ad ampio raggio la pubblica via e gli edifici circostanti e che solo una limitata porzione dell’area di ripresa include tale area di conferimento dei rifiuti, non potendosi, pertanto, il dispositivo video in questione considerarsi idoneo e proporzionato al più limitato obiettivo di monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti (v. già il provvedimento generale del Garante in materia di videosorveglianza dell’8 aprile 2010, doc. web n. 1712680, par. 5.4). Ciò fermo restando, quanto alla più generale finalità di tutela ambientale, che alcune recenti disposizioni introdotte dal legislatore nazionale prevedono un limitato utilizzo dei sistemi di videosorveglianza per l’accertamento di alcune residuali violazioni amministrative in materia di tutela ambientale (v. il d.l. 8 agosto 2025, n. 116, c.d. “Decreto terra dei fuochi”, convertito con la l. 3 ottobre 2025, n. 147, che ha novellato sia l’art. 255 del 3 aprile 2006, n. 152, Testo Unico Ambientale, sia l’art. 201 del Nuovo codice della strada, in relazione alle quali non è stato, peraltro, chiesto il prescritto parere del Garante previsto dall’art. 57, par. 1, lett. c), del Regolamento, riservandosi, pertanto, l’Autorità ogni valutazione in merito alla compatibilità di dette disposizioni con il quadro giuridico eurounitario e nazionale in materia di protezione dei dati).

Alla luce di tutte le considerazioni che precedono, non avendo il Comune identificato una chiara e valida base giuridica del trattamento, dotata dei necessari requisiti di rango e qualità, in relazione a ciascuna finalità di trattamento di natura amministrativa perseguita mediante dispositivi di videosorveglianza in questione, deve concludersi che il trattamento dei dati personali degli interessati (filmati di videosorveglianza e numeri di targa dei veicoli in sosta) risulta posto in essere in maniera non conforme al principio di “liceità, correttezza e trasparenza” e in assenza di base giuridica, in violazione degli artt. 5, par. 1, lett. a), 6, par. 1, lett. c) ed e), e parr. 2 e 3, del Regolamento, nonché 2-ter del Codice.

3.2. Il rispetto dei principi di minimizzazione dei dati e protezione dei dati fin dalla progettazione e per impostazione predefinita

Dall’istruttoria è emerso che la telecamera di videosorveglianza oggetto di reclamo era stata impostata in maniera tale da riprendere anche la facciata esterna della privata abitazione della reclamante, con visibilità di balconi, finestre e portefinestre (v. fotogramma sub all. 20-bis alla nota del Comune).

La ripresa di parte dell’abitazione della reclamante non può ritenersi “necessari[a]” (v. art. 6, par. 1, lett. c) ed e), del Regolamento) per il perseguimento di finalità di natura amministrativa o di sicurezza urbana, costituendo un’ingerenza sproporzionata nel diritto al rispetto della propria vita privata e familiare e alla protezione dei dati personali (v. artt. 8 CEDU e 7, 8 e 52 della Carta dei diritti fondamentali dell’Unione europea), che contrasta con la ragionevole aspettativa di riservatezza dei cittadini, specialmente con riguardo alle aree di proprietà privata, e ponendosi in contrasto con il richiamato principio di “minimizzazione dei dati” (art. 6, par. 1, lett. c), del Regolamento).

Nel rispetto dell’art. 25 del Regolamento, che formalizza il principio di “protezione dei dati fin dalla progettazione e protezione per impostazione predefinita”, i titolari del trattamento, proprio per prevenire trattamenti non conformi alla disciplina in materia di protezione dei dati, “devono mettere in atto adeguate misure tecniche e organizzative di protezione dei dati non appena pianificano l’installazione di un sistema di videosorveglianza, prima di iniziare la raccolta e il trattamento di filmati. Questi principi sottolineano la necessità di tecnologie integrate per il miglioramento della privacy, impostazioni predefinite che riducano al minimo il trattamento dei dati e l’adozione degli strumenti necessari ai fini della massima protezione possibile dei dati personali” (“Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video”, cit., par. 126; v. anche le “Linee guida 4/2019 sull’articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita”, adottate dal Comitato europeo per la protezione dei dati, del 20 ottobre 2020, spec. sez. 3.5).

Nel selezionare le opportune soluzioni tecniche, “il titolare del trattamento dovrebbe considerare le tecnologie che tutelano la privacy anche perché migliorano la sicurezza. Esempi di questo tipo di tecnologie sono i sistemi che consentono il mascheramento o l’offuscamento delle zone irrilevanti per la sorveglianza [...]” (“Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video”, cit., par. 129; ma v. già il citato provvedimento generale del Garante sulla videosorveglianza del 2010, ove si evidenziava che “l’attività di videosorveglianza [deve essere] effettuata nel rispetto del c.d. principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite (art. 11, comma 1, lett. d) del Codice”).

A tal riguardo, non possono essere prese in considerazione le ragioni meramente tecniche, logistiche e di opportunità addotte dal Comune per giustificare le modalità di configurazione dell’angolo di visuale della telecamera in questione.

D’altra parte, a seguito dell’apertura dell’istruttoria relativa al reclamo, il Comune ha fatto ricorso a una soluzione c.d. di “privacy masking” digitale, in maniera tale da oscurare la porzione dell’angolo di ripresa corrispondente alla privata abitazione della reclamante. Nell’ottica della minimizzazione e della protezione dei dati fin dalla progettazione (ma v. anche il già citato principio di proporzionalità nel previgente quadro normativo in materia di protezione dei dati), tale soluzione, tecnicamente percorribile, avrebbe dovuto essere, invece, attuata fin dalla prima configurazione e attivazione del sistema di videosorveglianza.

Deve, pertanto, concludersi che la condotta del Comune si è, altresì, posta in contrasto con i principi di “minimizzazione dei dati” e “protezione dei dati fin dalla progettazione e protezione per impostazione predefinita”, con conseguente violazione degli artt. 5, par. 1, lett. c) e 25 del Regolamento.

3.3. La trasparenza nei confronti degli interessati.

Nel rispetto del richiamato principio di “liceità, correttezza e trasparenza”, il titolare del trattamento deve adottare misure appropriate per fornire agli interessati, 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”, cit., in particolare par. 7; ma si veda già il “Provvedimento in materia di videosorveglianza” del Garante dell’8 aprile 2010, doc. web n. 1712680, in particolare par. 3.1; da ultimo, v. le FAQ del Garante in materia di videosorveglianza, cit., 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.

A tal riguardo, il Comune ha dichiarato di aver installato, in fase di prima configurazione dell’impianto di videosorveglianza, quattro cartelli informativi - dunque un numero esiguo rispetto alla complessiva aree del territorio comunale interessata dalla videosorveglianza - contenenti l’informativa di primo livello, non indicando, in ogni caso, l’esatta data di installazione degli stessi, avendo l’Ente confermato anche in sede di memoria difensiva che “con riferimento ai cartelli di primo livello originariamente posizionati, non risulta

possibile risalire alla data di loro installazione, che si presume essere coincidente con quella di attivazione del sistema di videosorveglianza. Non è possibile fornire ulteriori precisazioni in merito”.

Dalla documentazione in atti (v. all. 23) emerge anche l’inadeguatezza di tali cartelli, facendo gli stessi riferimento a generiche finalità di “sicurezza”, senza alcun riferimento alle finalità di natura amministrativa asseritamente perseguite e agli aspetti essenziali del trattamento, peraltro con rimando all’ormai abrogato art. 13 del Codice.

Tali cartelli sarebbero poi stati nel tempo comunque rimossi in occasione di lavori o altre non specificate esigenze.

Soltanto in data XX, dunque successivamente all’avvio dell’istruttoria relativa al reclamo, il Comune avrebbe installato dei “pannelli provvisori”, contenenti una nuova versione dell’informativa di primo livello, avviando “le procedure amministrative per la fornitura della cartellonistica definitiva”. Ciò trova conferma anche nelle dichiarazioni rese dal Comune con le proprie memorie difensive (“a seguito dell’avvio di istruttoria, il Comune ha richiesto al proprio DPO la trasmissione di un format completo di cartellonistica di primo livello, adeguata alle esigenze normative, da installare in via provvisoria nelle more dello svolgimento di apposite gare d’appalto per la fornitura della cartellonistica definitiva”).

Anche tale cartello provvisorio non risulta, tuttavia, pienamente conforme alla normativa in materia di protezione dei dati. In merito alle finalità di trattamento, esso indica, infatti, molteplici finalità di trattamento di carattere generiche ed eterogenee (“prevenire e reprimere atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, tutelare l’ordine, il decoro e la quiete pubblica, rilevare infrazioni al codice della strada, monitorare il traffico cittadino ed i relativi flussi, tutelare il patrimonio immobiliare e mobiliare dell’ente”), senza indicare in maniera puntuale la base giuridica a cui sarebbe riconducibile ciascuna distinta finalità di trattamento, erroneamente ingenerando nei cittadini la convinzione che qualsiasi condotta rilevante anche ai soli fini amministrativi possa essere accertata e contestata mediante il ricorso ai filmati di videosorveglianza. Nel cartello si fa, inoltre, menzione dei diritti dell’interessato in maniera sommaria, con riferimento al solo diritto di accesso, senza nemmeno un rimando alle pertinenti disposizioni del Regolamento (“è possibile accedere ai propri dati ed esercitare gli altri diritti riconosciuti dalla legge rivolgendosi al responsabile di videosorveglianza tramite PEC”). Inoltre, posto che non chiaro con quale figura coincida detto “responsabile di videosorveglianza”, il riferimento alla PEC, peraltro non indicata, come unico canale ammesso per l’esercizio dei diritti costituisce un’ingiustificata limitazione degli stessi. Quanto al periodo di conservazione dei dati, viene indicato un unico e indistinto periodo, pari a sette giorni, per tutte le molteplici e distinte finalità di trattamento, probabilmente mutuato dall’art. 6, comma 8, del d.l. 23 febbraio 2009, n. 11, che, tuttavia, trova applicazione esclusivamente in relazione alla finalità di tutela della sicurezza urbana e non, invece, necessariamente anche alle finalità aventi mera natura amministrativa.

Quanto all’informativa di secondo livello, il Comune ha dichiarato di aver pubblicato sul proprio sito web istituzionale un’informativa completa, dedicata dalla videosorveglianza, in una prima versione risalente al 2022 e in una successiva versione, redatta in concomitanza con la designazione del nuovo Responsabile della protezione dei dati, in data non specificata. Tali informative sarebbero state caricate in una pagina del sito web istituzionale, ma, a seguito dell’avvio dell’istruttoria, l’Ente si è accorto che il collegamento ipertestuale non era funzionante, ripristinando lo stesso in data XX.

Detta informativa sarebbe stata comunque consultabile online dal novembre 2022 al 20 giugno 2024.

Posto che l’informativa non è stata, pertanto, disponibile online in maniera continuativa per l’intero periodo di attivazione dell’impianto di videosorveglianza, la circostanza che non sia stata comprovata l’installazione, in numero sufficiente, di cartelli con l’informativa di primo livello, con una chiara menzione delle modalità di consultazione dell’informativa di secondo livello, pregiudica in radice l’efficacia del meccanismo di informativa stratificata su più livelli.

Peraltro, tale informativa, nelle due versioni prodotte in atti (v. all. 24 e 25), non risulta, in ogni caso, pienamente conforme alla disciplina di protezione dei dati. In particolare, quanto alle finalità di trattamento, esse fanno generico riferimento a “finalità strettamente connesse alla protezione delle persone e del patrimonio pubblico” e a non meglio specificate “finalità connesse ad obblighi previsti da disposizioni di leggi o regolamenti nazionali o sovranazionali, nonché da provvedimenti di enti o autorità, nazionali o

sovrnazionali”; indica erroneamente che “il trattamento potrà riguardare anche i dati particolari di cui all’art. 9 del Regolamento”; indica un unico tempo di conservazione dei filmati di videosorveglianza pari a sette giorni, che, come detto, trova applicazione soltanto all’ambito della sicurezza urbana; menziona erroneamente i diritti di rettifica e portabilità dei dati, non esercitabili con riguardo a filmati di videosorveglianza; individua erroneamente, nella prima versione del testo, il “responsabile del trattamento” nella persona del Segretario comunale.

Alla luce di tutto quanto sopra, deve concludersi che la condotta del Comune si pone in contrasto con il principio di “liceità, corretta e trasparenza” e in violazione degli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento.

3.4 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 residuo 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 “ogniquale volta 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 aver “adottato valutazione di impatto in data 30 luglio 2018, quando l’impianto si presentava già nella sua conformazione attuale” e che “il documento sarà stato oggetto di prossimo aggiornamento”.

A tal proposito, deve osservarsi che il Comune, al fine di comprovare tale dichiarazione, ha depositato in atti copia del verbale di deliberazione della Giunta comunale n. 52 del 30 luglio 2018. Nel presentare le proprie memorie difensive, l’Ente ha chiarito che “l’allegato 3 alla deliberazione di Giunta comunale n. 52 del 30 luglio 2018, in formato .xls, contiene la DPIA, che contempla esplicitamente i trattamenti in materia di videosorveglianza”, specificando che “il [...] foglio “DPIA Registro” [...] contiene la valutazione di impatto per ciascuna tipologia di trattamento, secondo il numero assegnato nel foglio precedente. La videosorveglianza è trattata al n. 20”. Pur prendendosi atto di tale circostanza, deve comunque osservarsi che il documento in questione, redatto in riferimento alla totalità dei trattamenti posti in essere dal Comune nell’ambito dello svolgimento delle proprie attività istituzionali, è del tutto inidoneo a soddisfare i requisiti previsti dall’art. 35 del Regolamento, prendendo lo stesso in considerazione, in una singola riga, la “videosorveglianza dei locali e/o della viabilità”, posta in essere mediante l’“apparato di videosorveglianza”, per la del tutto generica finalità di “sicurezza locali e delle vie”, in assenza di una puntuale “descrizione sistematica dei trattamenti previsti e delle finalità del trattamento” (art. 35, par. 7, lett. a), del Regolamento - es. numero di dispositivi video; illustrazione delle caratteristiche tecniche degli stessi; in assenza di una descrizione sistemi informatici per il salvataggio e la gestione dei filmati di videosorveglianza; riferimenti puntuali a ciascuna singola finalità di trattamento perseguito e alla relativa base giuridica, ecc.); in assenza di una “valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità” (art. 35, par. 7, lett. b), del Regolamento - es. numero di telecamere e siti di installazione scelti in relazione a ciascuna finalità di trattamento e allo specifico obiettivo di interesse pubblico perseguito; definizione dell’angolo di visuale; misure per evitare la ripresa di aree private o non necessarie; possibilità di ricorrere a misure alternative ma meno lesive per i diritti e le libertà degli interessati; ecc.); nonché in assenza di indicazioni circa le specifiche “misure previste per affrontare i rischi” prefigurati (art. 35, par. 7, lett. d), del Regolamento).

Tali lacune - che costituiscono al contempo il sintomo e il risultato di un approccio, da parte dell’Ente, solo formale ma non sostanziale all’adempimento previsto dall’art. 35 del Regolamento -, non consentono, pertanto, di poter qualificare tale documento, che nel tempo è stato soltanto “confermat[o]” (v. memoria

difensiva), come una valida valutazione di impatto sulla protezione dei dati, dovendosi, pertanto, considerare violata detta disposizione 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 di Arvier, per posto in essere un trattamento di dati personali, mediante dispositivi video, in violazione degli artt. 5, par. 1, lett. a) e c), 6, par. 1, lett. c) ed e), e parr. 2 e 3, 12, par. 1, 13, 25 e 35 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, par. 1, lett. a) e c), 6, par. 1, lett. c) ed e), e parr. 2 e 3, 12, par. 1, 13, 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.

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, tenuto conto che l'impianto di videosorveglianza comunale risulta essere attivo per il perseguimento di una pluralità di finalità di trattamento, 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; (ii) definire le specifiche finalità di trattamento di natura amministrativa eventuale perseguite mediante i dispositivi video in questione, rinvenendo un'idonea base giuridica che possa giustificare il trattamento per ciascuna di tali finalità; (iii) assicurare che l'angolo di ripresa di ciascuna telecamera non includa private abitazioni o altri luoghi pubblici o privati non d'interesse per il perseguimento di ciascuna finalità di trattamento, eventualmente adottando soluzioni tecniche di mascheramento o offuscamento; (iv) svolgere una valida e completa valutazione di impatto sulla protezione dei dati personali in relazione ai trattamenti posti in essere mediante sistemi di videosorveglianza; (v) riformulare 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.

6. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i e 83 del Regolamento; art. 166, comma 7, del Codice).

Il Garante, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso" e, in tale quadro, "il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, nel caso di specie la violazione delle disposizioni citate è soggetta all'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento.

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenendo in debito conto gli elementi previsti dall'art. 83, par. 2, del Regolamento.

Tenuto conto che:

- ancorché la violazione abbia avuto luogo per un esteso arco temporale, essa ha carattere colposo, essendo stata posta in essere per effetto di errate valutazioni sul piano giuridico da parte dell'Ente (cfr. art. 83, par. 2, lett. a) e b), 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 dimensione assai modeste (circa 800 abitanti), dotato, pertanto, di limitate risorse organizzative ed economiche, 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, anche adottando misure per rimediare alla specifica violazione oggetto di reclamo (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 4.000 (quattromila) per la violazione degli artt. 5, par. 1, lett. a) e c), 6, par. 1, lett. c) ed e), e parr. 2 e 3, 12, par. 1, 13, 25 e 35 del Regolamento, nonché 2-ter del Codice, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito Internet del Garante. Ciò in considerazione del fatto che il trattamento ha avuto luogo per un esteso arco temporale, senza assicurare la necessaria trasparenza nei confronti degli interessati e senza aver svolto una valida valutazione di impatto sulla protezione dei dati, peraltro sottoponendo a videosorveglianza una privata abitazione, in relazione alla quale sussiste un'elevata aspettativa di riservatezza da parte degli interessati.

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 Arvier per la violazione degli artt. 5, par. 1, lett. a) e c), 6, par. 1, lett. c) ed e), e parr. 2 e 3, 12, par. 1, 13, 25 e 35 del Regolamento, nonché 2-ter del Codice, nei termini di cui in motivazione;

ORDINA

al Comune di Arvier, in persona del legale rappresentante pro-tempore, con sede legale in Via Corrado Gex, 8 - 11011 Arvier (AO), C.F. 80003210079, di pagare la somma di euro 4.000 (quattromila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione. Si rappresenta che il

contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

al predetto Comune:

- in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 4.000 (quattromila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;
- ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, di conformare i trattamenti alle disposizioni del Regolamento, con le modalità indicate al par. 5 del presente provvedimento;
- 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 dell'Autorità;
- ai sensi dell'art. 17 del Regolamento del Garante n. 1/2019, l'annotazione delle violazioni e delle misure adottate in conformità all'art. 58, par. 2 del Regolamento, nel registro interno dell'Autorità previsto dall'art. 57, par. 1, lett. u) del Regolamento.

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

Roma, 23 settembre 2026

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Montuori