Gli approfondimenti di iSimply

Videosorveglianza comunale, il Garante alza l'asticella

Patto vigente, basi giuridiche chiare e DPIA preventiva. Le ultime ordinanze che impongono ai Comuni una verifica immediata dell'assetto

Ivrea, 9 febbraio 2026
di Enrico Capirone

Le più recenti ordinanze ingiunzione del Garante per la protezione dei dati personali in materia di videosorveglianza comunale, in particolare il provvedimento del 4 dicembre 2025 n. 730 rivolto al Comune di Tuscania e il provvedimento del 18 dicembre 2025 n. 752 rivolto al Comune di Nave, segnano un passaggio netto. Non si tratta di richiami formali o di irregolarità marginali, ma di decisioni che incidono direttamente sulla possibilità di continuare a utilizzare gli impianti, anche con misure correttive che possono arrivare al divieto di trattamento e alla cancellazione dei dati già raccolti.

Il messaggio che emerge è chiaro. La videosorveglianza, soprattutto quando è dichiarata a fini di sicurezza urbana o utilizza sistemi di lettura targhe e varchi LPR, non può più essere gestita come un insieme di dispositivi "tecnici" cui adattare ex post gli adempimenti privacy. È un trattamento complesso che richiede basi giuridiche verificabili, coerenza tra finalità dichiarate e configurazione reale dell'impianto, documentazione pronta e un governo unitario del sistema.

In particolare, le ordinanze insistono su tre snodi operativi:

- patto per la sicurezza urbana effettivamente vigente e riferibile all'impianto;
- finalità distinte con basi giuridiche puntuali;
- DPIA preventiva e coerente con le funzionalità reali.

In questo articolo ricostruiamo cosa comportano, in concreto, questi tre snodi e quali verifiche e adeguamenti prioritari servono per ridurre il rischio di rilievi, prescrizioni e blocchi operativi dell'impianto.

I link ufficiali ai due provvedimenti del Garante per la protezione dei dati personali, pubblicati sul sito istituzionale garanteprivacy.it (o gpdp.it):

- Provvedimento del 4 dicembre 2025 n. 730 (rivolto al Comune di Tuscania): https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10213467 (Include sanzione di 12.000 €, divieto su trattamenti lettura targhe, cancellazione dati e altre prescrizioni.)
- Provvedimento del 18 dicembre 2025 n. 752 (rivolto al Comune di Nave): https://www.garanteprivacy.it/garante/doc.jsp?ID=10213486 (Include sanzione di 6.000 €, violazioni multiple GDPR e prescrizioni su Patto sicurezza, DPIA, informative.)

Sommario

Sicurezza urbana e Patto: la linea è netta

Il Garante ribadisce con particolare fermezza che la videosorveglianza per finalità di sicurezza urbana è lecita solo se riconducibile alla disciplina di settore e, quindi, a un Patto per la sicurezza urbana stipulato con la Prefettura ai sensi dell’art. 5 del D.L. 14/2017. In assenza del Patto, o in presenza di un Patto scaduto o meramente generico, il trattamento non può essere ricondotto a quella finalità e resta privo di base giuridica adeguata.

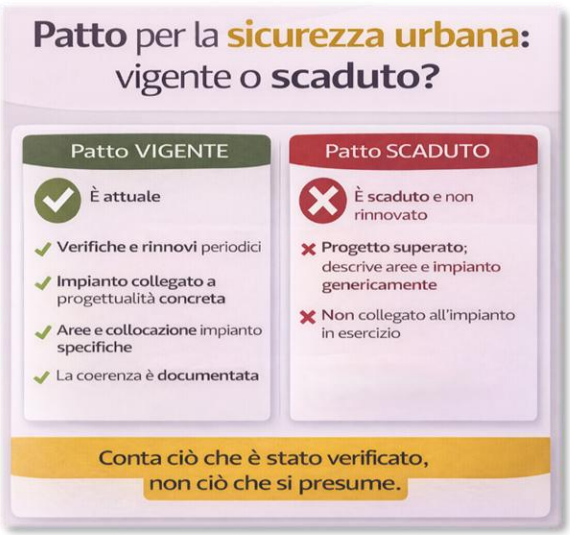
Non è sufficiente dichiarare di perseguire la sicurezza urbana, né richiamare competenze istituzionali in senso lato. Il Patto deve essere **vigente** e deve essere riferibile all’impianto realmente in esercizio.

In questa cornice, il Patto non può essere trattato come un documento “di archivio”. La sua utilità giuridica dipende dalla capacità di dimostrare che è attuale e riferibile all’impianto realmente in esercizio. Di conseguenza, conviene verificare in modo puntuale:

- che il Patto sia **vigente** al momento del trattamento e non **scaduto** o privo di rinnovo;
- che sia coerente con l’impianto oggi operativo e non con un progetto superato o parziale;
- che individui aree e logica di installazione in termini non generici;
- che il collegamento tra Patto e impianto sia riscontrabile anche nella documentazione interna e nella configurazione effettiva del sistema.

Attenzione: Patto scaduto = trattamento senza base giuridica per la finalità di sicurezza urbana

Nei provvedimenti del Garante l’assenza di un Patto vigente, o la presenza di un Patto non idoneo a descrivere l’impianto, comporta l’impossibilità di ricondurre il trattamento alla sicurezza urbana. In concreto, questo equivale a un trattamento privo di base giuridica, con rischio di divieto immediato e cancellazione dei dati.



Lettura targhe e varchi: non conta la narrazione, conta la configurazione

Un altro punto centrale riguarda l’uso dei sistemi di lettura automatizzata delle targhe. Il Garante non contesta in astratto la tecnologia, ma il modo in cui viene utilizzata.

Dalle istruttorie emerge uno schema ricorrente. I Comuni dichiarano che i varchi sono un “supporto alla contestazione immediata” o uno strumento di ausilio agli operatori. Tuttavia, i sistemi risultano configurati per funzionare in modo continuativo, registrando tutti i transiti, conservando i dati per giorni e interrogando banche dati esterne, indipendentemente dall’effettivo accertamento di un’infrazione.

Questo modello è ritenuto incompatibile con i principi di liceità, minimizzazione e limitazione della conservazione. Se il sistema registra tutti e “filtra dopo”, la violazione è già integrata. Un uso realmente puntuale richiede che la memorizzazione dei dati personali avvenga solo quando necessario e in coerenza con l’evento che giustifica il trattamento.

Finalità multiple e frammentate: un segnale di rischio

Entrambi i provvedimenti mettono in evidenza un problema tipico. La tendenza a cumulare, sullo stesso impianto, una pluralità di finalità eterogenee: sicurezza urbana, polizia giudiziaria, controllo del traffico, tutela ambientale, gestione dei rifiuti, monitoraggi statistici, supporto alla protezione civile.

Questa frammentazione rende difficile, se non impossibile, individuare basi giuridiche specifiche per ciascun trattamento. Quando l’impianto “serve a tutto”, spesso non è lecito per niente, perché manca

una chiara riconducibilità normativa e una separazione funzionale dei trattamenti.

Trasparenza reale, non solo cartelli

Le violazioni in materia di informativa non riguardano solo l’assenza o l’incompletezza dei cartelli. Il Garante censura in modo esplicito informative che:

- indicano finalità generiche;
- omettono trattamenti effettivamente svolti, come la classificazione ambientale dei veicoli o la comunicazione dei dati a soggetti terzi;
- rimandano a link errati o a informative non specifiche per la videosorveglianza.

Se un trattamento esiste ma non è descritto nell’informativa, la trasparenza è compromessa, anche in presenza di segnaletica visibile.

DPIA sempre necessaria

Il messaggio più operativo che emerge dalle ordinanze del 2025 è che la DPIA per la videosorveglianza comunale non è un adempimento accessorio. È un presidio sostanziale di conformità e accountability, rilevante anche ai fini della liceità in concreto e, soprattutto, di sostenibilità operativa dell’impianto. Nei casi dei Comuni di Tuscania e Nave, il Garante contesta l’avvio dei trattamenti in assenza di valutazione di impatto e ribadisce che, quando ricorre una sorveglianza sistematica su larga scala di aree accessibili al pubblico, la DPIA è obbligatoria ai sensi dell’art. 35 GDPR, in particolare dell’art. 35, par. 3, lett. c). Questo vale per la videosorveglianza stradale e di contesto e, a maggior ragione, per impianti che includono varchi e lettura automatizzata delle targhe, perché tali funzionalità aumentano la capacità del sistema di ricostruire spostamenti e comportamenti, con un impatto più elevato sui diritti degli interessati (provv. Tuscania 4 dicembre 2025, n. 730, doc. web n. 10213467, par. 3.3; provv. Nave 18 dicembre 2025, n. 752, doc. web n. 10213486, par. 3.3).

Questa impostazione non è un cambio improvviso di rotta, ma la prosecuzione di una linea già tracciata in modo netto. Nel provvedimento sul Comune di Levanto del 19 dicembre 2024 (doc. web n. 10107263) il Garante aveva già chiarito che, in presenza di un sistema esteso sul territorio comunale, la DPIA non può essere esclusa con valutazioni generiche o rassicurazioni interne. Deve essere preventiva, aderente all’impianto realmente configurato e capace di dimostrare necessità e proporzionalità delle scelte. In quel caso l’Autorità collega l’assenza di DPIA non solo a un difetto documentale, ma a una carenza strutturale di governance, perché senza DPIA l’ente non è in grado di dimostrare ex ante di aver governato rischi, configurazioni e accessi.

Nel 2025 il principio viene ulteriormente rafforzato e reso “praticabile” in istruttoria, perché il Garante neutralizza due difese ricorrenti che, nella prassi degli enti locali, continuano a riemergere:

- l’argomento della “tecnologia consolidata”, secondo cui l’uso di apparati diffusi o standardizzati renderebbe superflua la valutazione. La maturità tecnologica non incide sull’obbligo. Ciò che rileva è l’impatto del trattamento in termini di scala, continuità, finalità, capacità di identificazione e potenziale ricostruzione di comportamenti. Con varchi, LPR e controlli su banche dati esterne, la soglia di rischio tende a crescere, non a ridursi (provv. Nave, doc. web n. 10213486, par. 3.3);
- l’avvio tardivo della DPIA, dopo l’installazione o dopo l’attivazione dell’impianto. La valutazione di impatto deve precedere l’inizio del trattamento perché serve a orientare le scelte progettuali e configurative. Una DPIA redatta a posteriori non sana l’illiceità già maturata e non

dimostra che i rischi siano stati governati prima che l’impianto producesse effetti sugli interessati (provv. Tuscania, doc. web n. 10213467, par. 3.3 e conclusioni).

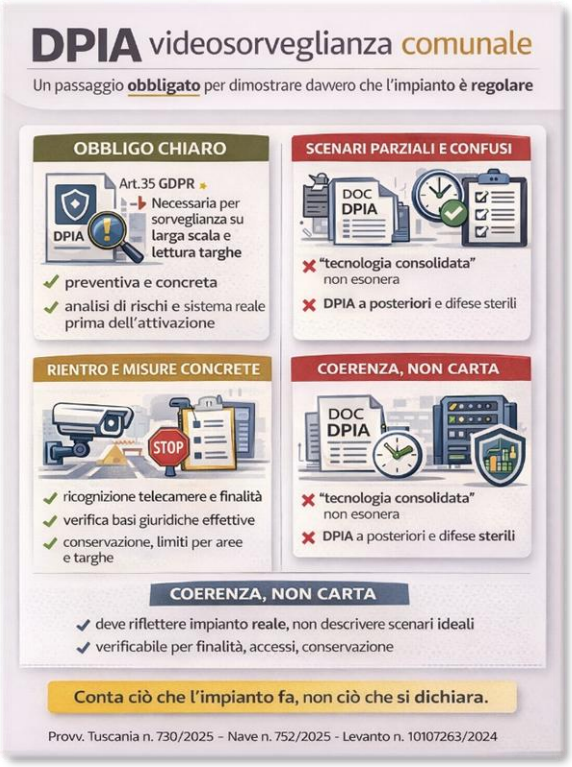
La conseguenza pratica è molto chiara per qualunque Comune che debba “regolarizzare” un impianto esistente. Se la DPIA non è stata svolta prima dell’attivazione, l’adeguamento non può ridursi a completare un modulo o a produrre un documento. Diventa un piano di rientro tecnico-organizzativo che può imporre la revisione delle finalità dichiarate, la separazione dei trattamenti, la riconfigurazione dei tempi di conservazione, la riduzione delle aree riprese e, nei casi più critici, la limitazione o disattivazione di funzionalità invasive. Non a caso, nei provvedimenti del 2025 la mancanza di DPIA è collegata a misure correttive “di sistema” come ricognizione dell’impianto, verifica delle basi giuridiche, revisione delle informative e, per la lettura targhe, anche divieto di trattamento e cancellazione dei dati già raccolti (provv. Tuscania, doc. web n. 10213467, misure correttive; provv. Nave, doc. web n. 10213486, misure correttive).

In termini di impostazione, la DPIA per videosorveglianza e varchi LPR diventa anche il contenitore obbligato per risolvere i nodi che più spesso determinano la contestazione del Garante, a partire dalla frammentazione delle finalità. Quando lo stesso impianto viene usato per sicurezza urbana, controlli di polizia stradale, tutela ambientale, rifiuti o finalità statistiche, una DPIA unitaria e generica è strutturalmente fragile. La valutazione deve scomporre il sistema in trattamenti distinti o, almeno, in configurazioni funzionali separabili, ciascuna con base giuridica specifica, regole di accesso e tracciamento, tempi di conservazione coerenti e misure di minimizzazione effettive.

Da ultimo, sul piano difensivo, la DPIA deve “fotografare” l’impianto reale. Se descrive un assetto ideale che non corrisponde alla configurazione effettiva, oppure omette funzionalità attive come memorizzazione generalizzata dei transiti o interrogazioni sistematiche, non solo non protegge l’ente. In istruttoria diventa un ulteriore fattore di rischio perché rafforza l’idea di un’accountability formale e non sostanziale, proprio il profilo che le ordinanze 2024-2025 stanno colpendo con maggiore nettezza.

DPIA: punto chiave

- In Comune, quasi sempre obbligatoria.
- Deve essere preventiva e aderente all’impianto reale.
- Tecnologia “consolidata” e DPIA tardiva non bastano.
- Se manca, serve un piano di rientro tecnico.
- Possibili stop e cancellazione dati.



Fornitori, accessi e catena delle responsabilità

Nei provvedimenti emergono criticità significative anche nella gestione dei fornitori e, più in generale, nella “catena” di soggetti che, a vario titolo, possono accedere al sistema o incidere sul trattamento. L’Autorità non guarda solo al fatto che l’impianto funzioni, ma pretende che l’ente sia in grado di dimostrare, in modo tracciabile, chi fa cosa, con quale titolo e con quali limiti. Quando contratti e designazioni sono incompleti, non coerenti con le attività svolte o non documentabili con data certa, l’intero assetto diventa fragile sotto il profilo dell’accountability e, di riflesso, della liceità e della sicurezza del trattamento.

Il punto operativo è che la nomina ex art. 28 GDPR non può essere trattata come un allegato “standard” o come un atto meramente formale. Deve riflettere la realtà tecnica e organizzativa del servizio: natura e finalità del trattamento, categorie di dati, durata, misure di sicurezza, regole su subfornitori, modalità di assistenza all’ente (anche rispetto a richieste degli interessati e incidenti di sicurezza), istruzioni documentate e limiti di accesso. Se il fornitore effettua manutenzione, teleassistenza, gestione credenziali, aggiornamenti software, hosting o backup, occorre che tali attività siano ricondotte in modo esplicito e coerente al perimetro contrattuale e alle istruzioni del titolare.

Accanto ai fornitori, pesa la gestione degli accessi. In istruttoria non basta affermare che “nessuno accede” o che “solo la Polizia Locale vede le immagini”. Occorre dimostrarlo con elementi verificabili: configurazioni di sistema, ruoli e profili autorizzativi, registro delle abilitazioni, procedure di

rilascio e revoca credenziali, segregazione dei privilegi, e soprattutto log di accesso e di consultazione dei filmati, conservati per un tempo congruo e effettivamente controllati. Se esistono credenziali “tecniche”, account condivisi, accessi remoti non governati o assenza di tracciamento, l’ente perde la capacità di provare il rispetto dei principi di minimizzazione e di integrità e riservatezza.

In pratica, la catena delle responsabilità si “rompe” quando manca evidenza documentale e tecnica su quattro passaggi essenziali: chi è responsabile del trattamento e per quali attività; chi può accedere e con quale profilo; quali operazioni sono possibili (visione, estrazione, esportazione, cancellazione); quali controlli esistono e come vengono verificati. Un impianto può essere anche ben progettato, ma senza contratti coerenti, ruoli chiari, log e procedure, diventa difficile difenderlo in caso di reclamo o ispezione e più esposto a prescrizioni correttive.

Diritti degli interessati: attenzione ai regolamenti comunali

Un ulteriore profilo critico riguarda la gestione delle istanze di accesso e cancellazione. È stato ritenuto illecito subordinare l’accesso alle immagini a una richiesta motivata o al pagamento di un contributo spese, sulla base di regolamenti comunali che mescolano accesso documentale e diritti privacy.

Se il regolamento sulla videosorveglianza prevede motivazione o costi per l’accesso ai dati personali, è un campanello d’allarme. Il diritto di accesso ai sensi degli artt. 12 e 15 GDPR non richiede giustificazione e deve ricevere risposta nei termini.

Misure correttive e rischio operativo

Le ordinanze non si limitano alla sanzione economica. Nei casi esaminati il Garante ha disposto:

- il divieto di proseguire i trattamenti relativi alla lettura targhe;
- la cancellazione dei dati già raccolti;
- la ricognizione completa di tutte le telecamere presenti sul territorio.

Questo significa che il rischio non è solo reputazionale o finanziario, ma operativo. Una funzione dell’impianto può essere fermata con effetto immediato.

Autovalutazione di conformità in 12 punti

Per una verifica rapida dell’assetto attuale, è utile rispondere “sì/no” a ciascun punto. La presenza di più risposte negative segnala un’esposizione concreta a rilievi, misure correttive e interruzioni operative, e rende opportuna una ricognizione formale con piano di adeguamento.

1. finalità dichiarate univoche e coerenti con l’uso reale dell’impianto;
2. base giuridica individuata e documentabile per ciascuna finalità;
3. impianto mappato e governato in modo unitario, senza “pezzi” fuori controllo;
4. varchi e lettura targhe configurati per minimizzare (no registrazione generalizzata dei transiti);
5. tempi di conservazione impostati e rispettati in modo verificabile;
6. informativa di primo livello completa e coerente con l’impianto in esercizio;
7. informativa di secondo livello effettivamente accessibile e aggiornata;
8. DPIA svolta prima dell’attivazione e aderente alle funzionalità effettive;
9. ruoli privacy e catena fornitori formalizzati e dimostrabili (art. 28, nomine, istruzioni);
10. accessi ai sistemi governati (profilazione, autenticazione forte, log, tracciabilità);
11. procedura DSAR operativa e compatibile con GDPR (no motivazioni/costi impropri);
12. evidenze di accountability pronte (registro trattamenti, audit/controlli, report e fascicolo privacy).

Se uno o più punti risultano negativi, gli scostamenti ricadono quasi sempre in alcuni errori ricorrenti già contestati dal Garante nei procedimenti più recenti, che sintetizziamo qui sotto come ‘errori tipici che costano cari’.

Errori tipici che costano cari

- Patto per la sicurezza urbana scaduto o non riferibile all’impianto attuale;
- uso continuativo dei varchi con registrazione generalizzata dei transiti;

- finalità eterogenee non separate né giustificate;
- informative incomplete o non aderenti ai trattamenti reali;
- DPIA assente o redatta dopo l’attivazione;
- regolamenti comunali che richiedono motivazione o costi per l’accesso alle immagini;
- contratti e nomine dei fornitori non dimostrabili;
- risposte istruttorie tardive o parziali.

Azioni da avviare entro 30 giorni

- verifica della vigenza del Patto e della sua coerenza con l’impianto attuale;
- mappatura delle finalità e dei trattamenti effettivi;
- controllo delle informative e della segnaletica;
- revisione delle procedure per la gestione dei diritti degli interessati;
- sospensione prudenziale delle funzionalità non chiaramente giustificate.

Azioni da completare entro 90 giorni

- ricognizione completa dell’impianto e dei fornitori;
- redazione o aggiornamento della DPIA;
- adeguamento dei contratti e delle nomine ex art. 28 GDPR;
- allineamento tra Patto, atti interni, configurazione tecnica e informative.

Le decisioni del Garante mostrano che la videosorveglianza comunale non è più tollerata come sistema “ibrido”, sostenuto da atti parziali e da prassi consolidate. Per Comandanti e Segretari comunali il punto non è difendere l’impianto esistente, ma **verificare se l’assetto attuale è realmente sostenibile**. Farlo ora consente di governare l’adeguamento. Rimandare significa esporsi a misure che non lasciano margini di gestione.

FAQ

Questo riguarda anche il nostro Comune se non abbiamo lettura targhe, ma solo telecamere di contesto?

Sì. La lettura targhe alza il rischio e rende più probabili misure correttive immediate, ma base giuridica, trasparenza, DPIA quando si riprende su larga scala e governance valgono anche per la videosorveglianza di contesto su pubblica via.

Se abbiamo un Patto per la sicurezza urbana siamo “coperti”?

Solo se il Patto è **vigente**, puntuale e coerente con l’impianto oggi in esercizio. Un Patto generico o un **Patto scaduto** non costituiscono una base giuridica valida per i trattamenti in corso.

Un Patto firmato anni fa è ancora valido?

Non automaticamente. Va verificata la durata prevista, l’eventuale rinnovo e la coerenza con l’impianto attuale. Un **Patto scaduto**, non rinnovato o riferito a un progetto diverso da quello oggi operativo non giustifica la prosecuzione della videosorveglianza per sicurezza urbana.

Il Patto è facoltativo perché il Sindaco è autorità locale di pubblica sicurezza?

Nei provvedimenti richiamati il Garante respinge questa impostazione quando si invoca la sicurezza urbana per la videosorveglianza. In assenza di **Patto vigente** o con **Patto scaduto**, la finalità di sicurezza urbana non è legittimamente sostenibile.

Se conserviamo i transiti solo 7 giorni, è sufficiente per la minimizzazione?

No, non basta. Conta anche se si registrano indiscriminatamente i transiti di tutti, indipendentemente dall’infrazione. La minimizzazione riguarda anche ciò che si raccoglie e quando lo si memorizza.

Possiamo usare la lettura targhe come “supporto” per controlli su assicurazione e revisione, se poi l’operatore verifica e contesta?

Il fatto che la decisione finale sia umana non elimina gli obblighi GDPR. Se il sistema registra in continuo e conserva transiti di tutti, servono basi giuridiche puntuali, minimizzazione, trasparenza e DPIA. L’assetto concreto fa la differenza.

Dobbiamo fare la DPIA sempre?

Nella videosorveglianza comunale, nella pratica, sì: è normalmente necessaria perché ricorre spesso una sorveglianza sistematica su aree accessibili al pubblico, e la DPIA deve precedere l’attivazione. Fa eccezione solo un numero limitato di casi in cui l’impianto è davvero circoscritto, non “su larga scala”, con configurazione minimizzata e senza funzionalità che aumentano la capacità di ricostruire spostamenti o comportamenti. Con sistemi di lettura automatizzata delle targhe, la DPIA è da considerare di fatto obbligatoria.

Basta un’informativa “generale” del Comune che include la videosorveglianza?

No. Serve un’informativa specifica, coerente con l’impianto reale e le finalità effettive, facilmente accessibile dai cartelli.

Il cartello può rimandare a una pagina generica o al sito del Garante?

No. Il cartello deve rimandare chiaramente alla pagina comunale corretta con l’informativa estesa. Un rimando errato compromette il meccanismo a due livelli.

Se il fornitore fa solo manutenzione, serve la nomina ex art. 28?

Se può accedere al sistema o alle immagini, anche potenzialmente, serve un inquadramento e un accordo adeguato. Se si sostiene che non accede, va reso vero e dimostrabile anche tecnicamente e organizzativamente.

Un cittadino deve motivare la richiesta di accesso alle immagini?

Per l’accesso ai dati personali non deve motivare. Il Comune deve gestire l’istanza nei termini e con risposte coerenti con GDPR.

Cosa rischiamo concretamente se siamo “fuori assetto”?

Dichiarazione di illiceità, sanzioni, pubblicazione del provvedimento, ingiunzioni di adeguamento e, nei casi più critici, limitazione o divieto del trattamento e ordini di cancellazione dei dati, soprattutto sui dati di targa.

Qual è il primo passo pragmatico per ridurre subito il rischio?

Verificare subito se il Patto è **vigente** o **scaduto**, mappare impianto e finalità reali e intervenire su ciò che genera raccolta indiscriminata, soprattutto varchi lettura targhe continui e conservazione generalizzata, poi completare DPIA e trasparenza.