

Comune di Trezzano sul Naviglio



Città Metropolitana di Milano

**PROGETTO
DI DEFINIZIONE STRATEGICA E NORMATIVA
DELL'IMPIANTO DI VIDEOSORVEGLIANZA
COMUNALE CON IMPIEGO DI NUOVE
TECNOLOGIE DEDICATO ALLA SICUREZZA
URBANA INTEGRATA**

**Contrasto dell'attività predatoria e
potenziamento della sicurezza locale**

LEGGE N. 48/2017

STRATEGIE PER L'INNOVAZIONE DELLA SICUREZZA URBANA INTEGRATA

Elaborato

Redatto da

Rev . **1.0**

Del **01.06.2026**

Rapp:

Stefano Manzelli – Consulente Enti Locali e Forze Di Polizia

Validazioni

Il Responsabile

PREMESSA

La videosorveglianza cittadina è un tema in forte espansione ed è una prerogativa necessariamente gestita dai comuni che ai sensi dell'art. 6 del dl 11/2009 (e del dl 116/2025) possono utilizzare gli impianti per la tutela della sicurezza urbana, stradale e ambientale, riprendendo le strade e le piazze. La riforma sovranazionale sulla tutela dei dati personali ha rinnovato tutte le regole stabilendo in buona sostanza che spetta al titolare del trattamento assumersi ogni responsabilità ed essere in grado di rendicontare le proprie scelte (accountability). Gli impianti di videosorveglianza pubblica servono però generalmente anche ad una finalità di sicurezza in senso stretto. Dopo la firma di appositi patti in prefettura, infatti, i sindaci possono mettere a disposizione anche di polizia di Stato e carabinieri gli impianti di telecontrollo. Ecco allora che entra in gioco oltre al GDPR la poco conosciuta direttiva Ue 2016/680 che è stata attuata in Italia con il dlgs 51/2018. E tra poco, progressivamente, il regolamento Ue 2024/1689 sull'intelligenza artificiale e una serie di norme sulla cybersicurezza estremamente severe e complesse. Senza un'adeguata valutazione organizzativa, a partire da un robusto regolamento sulla videosorveglianza, il rischio per il titolare del trattamento è per esempio di non riuscire a gestire le richieste di esercizio dei diritti dell'interessato. Oppure di non poter attivare serenamente i collegamenti con polizia e carabinieri. Attenzione poi alla necessarie valutazioni di impatto privacy. Ogni moderno impianto di videosorveglianza urbana deve essere analizzato in modo da verificare preventivamente, dal punto di vista del cittadino, quali sono i rischi che emergono. Ovvero se il rischio individuato è accettabile o meno. Senza questi certificati ogni impianto di videosorveglianza è potenzialmente a rischio di sanzione. Quindi per un ente locale che vuole regolarizzare un sistema di videosorveglianza è necessario:

- 1) un regolamento e gli atti esecutivi che regolino nel dettaglio tutti gli aspetti organizzativi;
- 2) un patto per la sicurezza dettagliato per aprire alla corretta collaborazione interforze;
- 3) una o più valutazioni di impatto privacy (dpia) che attestino la conformità dell'impianto.

L'algoritmo dell'Accountability* per la videosorveglianza urbana integrata



*fonte F. Pizzetti e AAVV, Protezione dei dati in Italia tra Gdpr e codice novellato

1. INTRODUZIONE

Il comune di Trezzano sul Naviglio ha la necessità di strutturare un dettagliato progetto strategico di materia di videosorveglianza urbana integrata finalizzato alla regolarizzazione formale, privacy by design, degli impianti di videosorveglianza, in sincronia con la riforma della privacy (Regolamento Ue 2016/679, Codice privacy e dlgs 51/2018), nel rispetto del D.L. 14/2017, del D.L. 116/2025, del reg. Ue 2024/1689 e delle disposizioni sulla cybersecurity.

Il presente progetto strategico viene redatto sulla base della determina n. 200 del 13 marzo 2026 redatta dal comando di polizia locale ed avente per oggetto affidamento del servizio di supporto strategico triennale finalizzato alla regolarizzazione dei sistemi integrati di videosorveglianza e degli atti di regolamentazione e di condivisione dei dati, nonché alla redazione di un nuovo patto per la sicurezza urbana da attivarsi attraverso:

- La realizzazione di un progetto strategico per l'inquadramento degli impianti;
- Supporto alla regolarizzazione della privacy per la videosorveglianza;
- Supporto alla formalizzazione dei rapporti interforze;
- Supporto alla redazione della DPIA.

Scopo di questo documento è, quindi, innanzitutto, la descrizione dello stato di fatto giuridico - normativo complessivo su cui si posa un moderno progetto di sicurezza urbana integrata anche alla luce della recente riforma della tutela dei dati personali e la predisposizione di una architettura funzionale di sistema evoluto interforze di videocontrollo urbano da presentare alla prefettura per i successivi adempimenti formali finalizzati ad attivare:

- 1) il potenziamento della sicurezza urbana;
- 2) il controllo interforze;
- 3) la regolazione dei processi privacy.

La presente proposta di architettura progettuale, debitamente approvata nelle sedi opportune, potrà essere affiancata dalla realizzazione di un progetto tecnico vero e proprio affidato ad un tecnico progettista abilitato.

La stessa si fonda sulla necessità insuperabile di salvaguardare le diverse finalità e prerogative della polizia locale e delle altre forze di polizia dello Stato ovvero:

Per la polizia locale: sarà necessario utilizzare il sistema per finalità di sicurezza urbana stradale e ambientale, ai sensi dell'art. 6 del dl 11/2009 e del dl 116/2025 con condivisione delle segnalazioni sui transiti di veicoli da controllare con conservazione dei dati consentita per un periodo non inferiore a 7 giorni sui server di proprietà comunale (almeno 90 gg per i varchi ocr per finalità di sicurezza stradale e 15 gg per le fototrappole), con titolarità del trattamento dei dati personali in capo al comune.

Per le altre forze di polizia: sarà possibile utilizzare lo stesso sistema per le finalità di sicurezza e ordine pubblico con eventuale condivisione delle segnalazioni sui transiti di veicoli rubati e da controllare, su un ambito territoriale allargato, con titolarità del trattamento dei dati personali in capo al Ministero dell'interno e al Comando Generale dell'Arma dei Carabinieri ed altri eventuali soggetti istituzionali.

2. LA SICUREZZA DELLE CITTA'

Con l'entrata in vigore del dl 14/2017 l'architettura della sicurezza urbana è stata sottoposta ad un decisivo intervento di riforma che avrà profonde ricadute anche sulla gestione del comparto sicurezza. Per i sindaci in questi anni è stato infatti inevitabile chiedere alla polizia municipale di garantire un maggior controllo del territorio mettendo a disposizione le migliori tecnologie e tutte le risorse umane disponibili. Questa indicazione proveniente dall'esperienza territoriale è stata trasfusa nel dl 14/2017, convertito nella legge n. 48/2017. Il provvedimento è particolarmente innovativo perché per la prima volta sono state formalizzate le pratiche operative sperimentate da anni in varie località differenziando il concetto di sicurezza integrata rispetto a quello di sicurezza urbana. Per **sicurezza integrata** ai sensi del dl 14/2017 si intendono tutti gli interventi assicurati dallo Stato, dalle regioni e dagli enti locali per concorrere, nel rispetto delle diverse competenze, alla promozione di un sistema unitario ed integrato di sicurezza. Raccogliere e gestire in maniera uniforme le informazioni, le pratiche operative, condividere la gestione degli strumenti tecnologici di contrasto della criminalità e dell'attività predatoria tra polizia locale, polizia di Stato, carabinieri ecc. rappresentano gli obiettivi qualificanti della riforma. Per promuovere efficacemente queste nuove politiche di controllo del territorio il 24 gennaio 2018 la Conferenza unificata ha diramato le **linee generali** delle politiche pubbliche per la promozione della sicurezza integrata. L'atteso documento sancisce il via libera a tutta una serie dettagliata di iniziative conseguenti e soprattutto permetterà agli enti locali di sottoscrivere nuovi patti per la sicurezza urbana aggiornati alle conseguenti **linee guida** che sono state approvate il 26 luglio 2018. La **sicurezza urbana**, nel frattempo, è stata riformulata dal dl 14/2017, all'art. 4 e meglio definita come "il bene pubblico che afferisce alla vivibilità e al decoro delle città da perseguire anche attraverso interventi di riqualificazione e recupero delle aree o dei siti più degradati, l'eliminazione dei fattori di marginalità e di esclusione sociale, **la prevenzione della criminalità, in particolare di tipo predatorio**" da potenziare con l'uso degli strumenti pattizi (sindaco – prefetto) ispirati ad una logica di gestione consensuale ed integrata della sicurezza.

FASE
A

L'INQUADRAMENTO TEORICO GENERALE

LA VIDEOSORVEGLIANZA COMUNALE, TIPICAMENTE FINALIZZATA ALLA TUTELA DELLA SICUREZZA URBANA AI SENSI DEL DL 11/2009 (E ORA IBRIDA EX DL 116/2025), ASSUME ANCHE UNA POSSIBILE CONNOTAZIONE INTERFORZE. IN OGNI CASO LE ATTITUDINI DEL TRATTAMENTO DEVONO ESSERE IDENTIFICATE VALUTANDO:

- 1) LA LICEITA'
- 2) LE FINALITA'
- 3) LA NECESSITA'
- 4) LA TRASPARENZA
- 5) LA CORRETTEZZA
- 6) LA CONSERVAZIONE
- 7) GLI EVENTUALI RAPPORTI INTERFORZE

3. I PATTI PER LA SICUREZZA SINDACO - PREFETTO

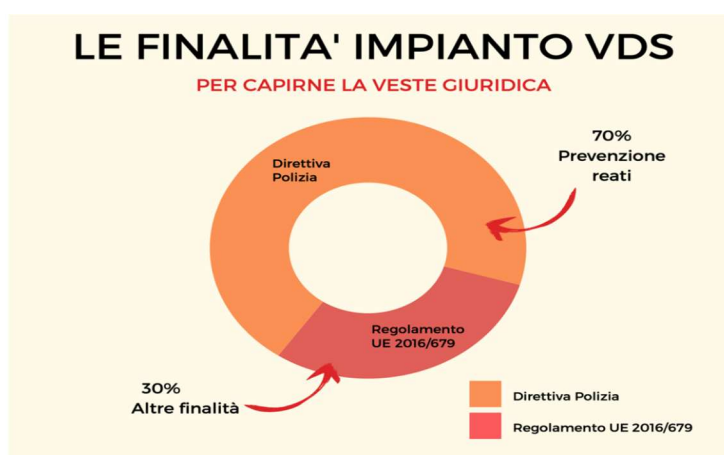
Con le linee generali del 24 gennaio 2018 il pacchetto sicurezza Minniti (dl 14/2017) ha subito una brusca accelerazione. Era, infatti, necessario definire la cornice organica degli strumenti attraverso i quali i diversi livelli di governo ma anche i soggetti privati sono chiamati a cooperare per realizzare l'integrazione delle politiche che hanno come obiettivo l'innalzamento dei livelli di sicurezza. Le linee generali specificano che in ogni caso saranno i prefetti a dover coordinare gli interventi di potenziamento e miglioramento degli impianti di video controllo, in un'ottica di sicurezza integrata, avvalendosi del Comitato provinciale per l'ordine e la sicurezza pubblica. Le successive linee guida approvate il 26 luglio 2018 dalla Conferenza Stato – città ai sensi del decreto Minniti n. 14/2017 stabiliscono la cornice di riferimento per ogni progetto da realizzare in materia di sicurezza urbana; in particolare definiscono la traccia per i patti per la sicurezza che devono essere sottoscritti tra sindaco e prefetto prima di dare seguito a qualsiasi iniziativa anche in materia di videosorveglianza. I patti per la sicurezza, ai sensi dell'art. 5 del dl 14/2017, potranno essere di carattere generale o specifici per singole questioni ed in ogni caso dovranno essere approvati dal comitato provinciale per l'ordine e la sicurezza e successivamente validati dal Viminale. In pratica, il patto per la sicurezza è un documento strategico fondamentale per il territorio che deve essere sottoscritto tra il primo cittadino e il rappresentante governativo per orientare le scelte fondamentali in materia di sicurezza urbana integrata, ma che di fatto condiziona anche le finalità e i mezzi in materia di tutela del trattamento dei dati personali facendo intravedere all'interprete, fin da questa fase, la predisposizione di una inevitabile convergenza privacy verso accordi di contitolarità (o comunque di convergenza delle finalità) tra forze di polizia locale e dello Stato. Uno specifico filone di intervento riguarda il ricorso agli strumenti di videosorveglianza. La cooperazione tra polizia locale, carabinieri e polizia di Stato trova, infatti, con questi strumenti un'attuazione concreta e molto diffusa. Per questo motivo l'accordo incoraggia il potenziamento e il miglioramento di queste tecnologie, "ai fini dell'utilizzo in comune degli apparati".

4. LA NUOVA STAGIONE DELLA SICUREZZA URBANA

Formalmente per sicurezza urbana ora si intende, ai sensi del dl 14/2017, *"Il bene pubblico che afferisce alla vivibilità e al decoro delle città, da perseguire anche attraverso interventi di riqualificazione e recupero delle aree o dei siti più degradati, l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio, la promozione del rispetto della legalità e l'affermazione di più elevati livelli di coesione sociale e convivenza civile, cui concorrono prioritariamente, anche con interventi integrati, lo Stato, le Regioni e Province autonome di Trento e di Bolzano e gli enti locali, nel rispetto delle rispettive competenze e funzioni"*. Anche se la definizione appare poco snella è evidente che la sicurezza urbana attiene anche al contrasto dei reati e quindi ad attività di prevenzione e di polizia in senso lato. Il tema più importante da esplorare ai fini della presente ricerca è il rapporto tra l'istituto della sicurezza urbana, di competenza dei comuni, e l'istituto dell'ordine e della sicurezza pubblica, di stretta pertinenza dello Stato, e della conseguentemente interferenza operativa e funzionale in materia di videosorveglianza urbana integrata tra polizia locale e polizia dello Stato. Riprendendo la precedente decisione n. 285/2019, la Corte Costituzionale, con la recente sentenza n. 236 del 21 ottobre 2020, ha ribadito che l'ordine pubblico e la sicurezza sono funzioni primarie che "costituiscono una materia in senso proprio e cioè una materia oggettivamente delimitata rispetto alla quale la prevenzione e repressione dei reati costituisce uno dei nuclei essenziali; materia che peraltro non esclude l'intervento regionale in settori ad essa liminari dovendosi in proposito distinguere tra un nucleo duro della

sicurezza di esclusiva competenza statale definibile quale sicurezza in senso stretto (o sicurezza primaria), e una sicurezza in senso lato (o sicurezza secondaria), capace di ricomprendere un fascio di funzioni intrecciate, corrispondenti a plurime e diversificate competenze di spettanza anche regionale”.

La sicurezza urbana (o sicurezza secondaria) è sempre più assimilabile alla sicurezza pubblica (meglio definita come sicurezza primaria). Questa complementarità interferisce con la corretta individuazione anche dei ruoli privacy in particolare se si tratta di utilizzare strumenti condivisi. Da una parte infatti abbiamo una norma che precisa come per la tutela della sicurezza urbana i comuni possono utilizzare i sistemi di videosorveglianza. Dall'altra provvedimenti normativi dedicati solo alle forze di polizia dello Stato. Fino al 25 maggio 2018 non c'era dubbio che polizia locale e forze di polizia dello Stato, in qualità di titolari autonomi, perseguissero finalità differenti. Con l'entrata in vigore della riforma sulla tutela dei dati ed in particolare del D.lgs. 51/2018 che ha recepito la direttiva polizia il panorama di riferimento è variato. Chiunque svolga funzioni di prevenzione dei reati e degli illeciti amministrativi deve allineare il trattamento dei dati personali sia al Gdpr che al D.lgs. 51/2018.



Nel corso degli ultimi anni l'Autorità ha inserito in alcuni ripetuti provvedimenti sanzionatori una indicazione "innovativa" ovvero che i patti per la sicurezza sindaco-prefetto sono sempre necessari per legittimare l'attivazione di telecamere comunali per il contrasto dell'attività predatoria. Ovvero per l'installazione di telecamere dedicate alla sicurezza urbana (che ai sensi del dl 14/2017 ora ricomprende "la prevenzione della criminalità, in particolare di tipo predatorio"). Specifica ad esempio il provvedimento 19 dicembre 2024, n. 805, adottato dal Garante a carico del comune di Levanto (confermato con il prov. 628 del 23/10/2025 a carico del comune di Curtarolo e con il provvedimento n. 669 del 13/11/25 adottato a carico del comune di Orte, poi a seguire con i provvedimenti nn. 730/25 e 752/25 a carico rispettivamente dei comuni di Tuscania e Nave) **"che la disciplina di settore consente ai comuni l'impiego di telecamere di videosorveglianza ai soli fini di prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria, previa stipula di un accordo per l'attuazione della sicurezza urbana con la prefettura territorialmente competente" con elenco dettagliato di tutti i device attivi**. Questa indicazione, letteralmente, mette in discussione il dettato normativo previsto dall'art. 6/7° del decreto legge n. 11/2009 il quale dispone che "per la tutela della sicurezza urbana, i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico". Ma anche l'istituto stesso del patto per la sicurezza, disciplinato dall'art. 5 del dl 14/2017, che nasce per favorire la leale collaborazione interistituzionale. In attesa di chiarimenti sui ruoli

quindi meglio sollecitare le prefetture alla sottoscrizione dei patti e finalizzare l'impiego dei dispositivi di videosorveglianza tipo lettura targhe alla finalità della sicurezza stradale.

5. PRIVATI E VIDEOSORVEGLIANZA

A Torino i privati potranno posizionare telecamere direttamente sulle strade previo accordi vincolanti con il comune. Sostenendo i costi ma perdendo di fatto la disponibilità dei filmati. Con la deliberazione di Giunta n. 510 del 2 settembre 2025, la Città di Torino ha introdotto un modello di videosorveglianza partecipata che consente a cittadini, associazioni e operatori economici di contribuire al potenziamento del sistema comunale, senza però poter accedere direttamente alle immagini. Il meccanismo si fonda sull'acquisto e messa a disposizione da parte dei privati di telecamere tecnologicamente avanzate, integrate nella rete comunale e gestite in via esclusiva dal comune, titolare del trattamento. L'iter prevede la presentazione di un progetto tecnico a carico del privato e la valutazione di idoneità da parte del municipio. La stipula di una convenzione approvata dalla Giunta con obbligo per il privato di sostenere i costi di installazione, manutenzione, connessione, storage dei dati e licenze software, nonché di adeguare la segnaletica. La cornice normativa è delineata dal dl 14/2017, art. 7, che consente la partecipazione dei soggetti privati a progetti di sicurezza urbana mediante accordi o patti locali con specifiche agevolazioni fiscali per chi investe in sistemi avanzati dotati di analisi video e invio automatico di allarmi alle centrali operative. Il regolamento comunale torinese disciplina in dettaglio modalità e criteri di valutazione dei progetti. Una volta approvati, gli impianti sono interamente gestiti dal comune, che assume anche la responsabilità privacy. Se da un lato il modello consente di ampliare senza costi diretti il patrimonio tecnologico pubblico, dall'altro presenta criticità evidenti. Il privato non può legittimamente monitorare la pubblica via e difficilmente sarà incentivato a sostenere oneri così gravosi per un beneficio solo indiretto. In prospettiva, una soluzione più sostenibile potrebbe essere rappresentata dall'impiego di sistemi "stand alone", messi a disposizione in via esclusiva delle forze di polizia, che garantiscono un bilanciamento più efficace tra sicurezza urbana, investimenti e tutela della riservatezza.

6. VIDEOSORVEGLIANZA E CODICE DELLE TELECOMUNICAZIONI

L'installazione e l'esercizio dei sistemi di videosorveglianza urbana da parte degli enti locali è considerata attività libera ai sensi del codice delle comunicazioni, ma solo se il comune ha sottoscritto un patto per la sicurezza urbana integrata finalizzato al contrasto dell'attività predatoria e della criminalità assieme al prefetto. Lo ha evidenziato l'art. 38/3° del dl 16 luglio 2020, n. 76 contenente misure urgenti per la semplificazione e l'innovazione digitale il quale specifica che "l'installazione e l'esercizio di sistemi di videosorveglianza di cui all'art. 5, comma 2, lettera a), del decreto legge 20 febbraio 2017, n. 14, convertito con modificazioni, dalla legge 18 aprile 2017, n. 48, da parte degli enti locali, è considerata attività libera e non soggetta ad autorizzazione generale di cui agli articoli 99 e 104 del decreto legislativo 1° agosto 2003, n. 259". Ma solo se si tratta degli impianti finalizzati alla tutela della sicurezza urbana integrata. Ovvero degli impianti di videosorveglianza preferibilmente condivisi con tutte le forze di polizia che siano stati adeguatamente considerati in un patto per la sicurezza ad hoc sottoscritto tra il sindaco e il prefetto per un miglior contrasto dell'attività predatoria e della criminalità diffusa.

7. IMPIANTI LETTURA TARGHE UFFICIALI: SCNTT

Attualmente l'unico modo "ufficiale" per attivare una fattiva collaborazione interforze sui veicoli rubati tra polizia locale e forze di polizia dello Stato, nel rispetto delle diverse prerogative, con uso condiviso dei sistemi evoluti di videosorveglianza urbana, risulta quello di costruire un percorso formale ben articolato e strutturato, anche in riferimento al codice

privacy, finalizzato a permettere un adeguato bilanciamento delle esigenze operative di tutti gli attori coinvolti. Da una parte la polizia locale, con imprescindibili esigenze di sicurezza urbana, stradale e di protezione passiva del personale operante (in caso di rintraccio di veicoli rubati o utilizzati da malviventi), dall'altro le forze di polizia dello Stato e l'autorità giudiziaria, con evidenti interessi investigativi di sicurezza e di ordine pubblico. Con la circolare del 12 gennaio 2018 il dipartimento di pubblica sicurezza del ministero dell'interno ha ben evidenziato questa necessità progettuale. Secondo le precedenti direttive impartite dal Viminale con la circolare n. 558/sicpart/421.2/70 del 2 marzo 2012, specifica la nota, i progetti di realizzazione dei sistemi di lettura targhe "gestiti dalle amministrazioni comunali devono essere oggetto di valutazioni in sede di Comitato provinciale per l'ordine e la sicurezza pubblica, volte all'approvazione delle caratteristiche infrastrutturali (ubicazione del sistema centrale e dei dispositivi di lettura targhe sul territorio) e dell'eventuale interconnessione primaria verso i sistemi di acquisizione dislocati presso gli uffici territoriali della polizia di Stato. A valle di tali valutazioni, qualora si intenda procedere all'ulteriore riversamento dei dati acquisiti con i suddetti sistemi di lettura targhe nella banca dati del sistema Scntt, ospitato presso il centro elettronico nazionale della polizia di stato sito in Napoli, dovrà essere inoltrata esplicita richiesta a questa direzione centrale, corredata dalla documentazione tecnica che descrive le modalità di interconnessione. Gli interventi tecnici per realizzare l'effettiva interconnessione all'Scntt dovranno essere eseguiti secondo le specifiche tecniche allegate, con il supporto e l'approvazione delle zone telecomunicazioni territorialmente competenti, di concerto con il centro elettronico nazionale ed il 5° settore dell'ufficio per i servizi tecnico gestionali della segreteria del dipartimento della pubblica sicurezza. Ciò premesso si rappresenta che il sistema Scntt è stato regolamentato normativamente dal Dpr 15/2018 che individua il trattamento dei dati effettuati dalle forze di polizia in attuazione dell'abrogato art. 53 del codice per la protezione dei dati personali: l'Scntt prevede, infatti, un trattamento dei dati - relativo al transito degli autoveicoli acquisiti attraverso telecamere dedicate, (...) trasmessi a server allocati presso gli uffici periferici della polizia di stato ed a loro volta, inviati presso la banca dati del Cen, finalizzato ad attività di sicurezza pubblica, nonché all'accertamento o alla repressione dei reati a supporto delle indagini di iniziativa o delegate dall'autorità giudiziaria.- L'architettura dello stesso, realizzata in modalità distribuita, prevede che i server periferici di gestione dei transiti (license plate recognition – lpr) siano ubicati presso gli uffici di polizia (questure, zone tlc, ecc) ed interconnessi in termini di flussi dati e funzionalità con la banca dati ubicata presso il Cen. A tale proposito, considerata la sensibilità dei dati trattati, è opportuno che in fase di valutazione dell'architettura dei sistemi, il Comitato provinciale per l'ordine e la sicurezza pubblica presti particolare attenzione ai seguenti punti: - il sistema deve consentire di distinguere i profili autorizzativi delle diverse utenze, al fine di controllare l'insieme di informazioni visibili in base alla competenza istituzionale dell'utilizzatore (forze di polizia a competenza generale, polizie locali ecc); - prima dell'avvio in esercizio del sistema, è necessario definire formalmente i ruoli e le responsabilità di tutti i soggetti a diverso titolo coinvolti, dove siano descritte le finalità che si intende perseguire e la loro gestione operativa, coerentemente con la normativa in tema di protezione dei dati personali". Per tentare di agevolare questi complessi rapporti interforze il ministero mette a disposizione degli interessati un fac-simile di protocollo di intesa, da utilizzare come modello.

8. ATTENZIONE AGLI OCR E ALLE LISTE INTERFORZE

I comuni che installano telecamere per la lettura delle targhe devono ottenere il nulla osta della Prefettura ovvero annotare questi device nei patti per la sicurezza. Diversamente questi dispositivi non potranno essere utilizzati per le consuete finalità di prevenzione dei reati. Lo ha evidenziato il Garante per la protezione dei dati personali con il provvedimento n. 10107263 del 19 dicembre 2024, sanzionando un comune ligure. L'ente aveva installato

numerose telecamere tra cui alcune specificamente preposte alla lettura delle targhe dei veicoli al fine di monitorare i flussi di traffico, analizzare le caratteristiche dei veicoli e verificarne la regolarità amministrativa. Tuttavia il trattamento dei dati è risultato privo di un'adeguata base giuridica, con tempi di conservazione illegittimi, informative non conformi e mancanza di una valutazione di impatto. L'istruttoria è partita da un articolo di stampa che segnalava il sistema di sorveglianza, confermato poi dal Comune sul proprio sito istituzionale. Il sistema comprendeva 121 telecamere, di cui sei con lettura targhe, utilizzate per raccogliere informazioni su provenienza, classe ambientale e caratteristiche dei veicoli. Il comune ne evidenziava anche la valenza investigativa, dichiarando che le immagini potevano supportare le indagini su furti e incidenti. Tuttavia, l'uso di questi dispositivi senza un patto per la sicurezza che ne ammettesse l'impiego ha reso il trattamento dei dati illecito. In mancanza di un patto quindi meglio finalizzare questi trattamenti alla sicurezza stradale. Ma con il provvedimento n. 752 del 18 dicembre 2025 adottato a carico del comune di Nave anche questa indicazione non sembra sufficiente. Per il Garante anche per gli ocr dedicati al controllo stradale sembra essere sempre necessario un patto per la sicurezza ad hoc. Anzi se il patto non indica in maniera dettagliata quali device sono presenti a parere del Garante l'impianto comunale rischia di essere sanzionato. Con il successivo provvedimento adottato a carico del comune di Mazzara del Vallo n. 102 del 12 febbraio 2026 l'Autorità si è spinta oltre censurando anche l'uso errato di questi lettori per l'invio massivo di violazioni per mancata revisione e copertura assicurativa senza contestazione immediata. Ma resta sempre sul tappeto il "problema dei problemi". Ovvero l'uso smodato delle liste interforze senza alcuna formalità e con l'impiego di sistemi tipo telegram. Anche se qualche prefettura sta adottando degli interessanti protocolli come quello sottoscritto a Brescia il 27 maggio 2025, manca una indicazione univoca centrale. In pratica anche in presenza di un accordo locale o al limite di un atto amministrativo generale che ammetta temporaneamente la comunicazione tra titolari autonomi dei dati catturati per le stesse finalità si consiglia di richiedere ai fornitori dei servizi di gestione dei varchi di abilitare utenze master differenziate tra forze di polizia locale e dello stato per permettere una segmentazione delle responsabilità. Ovvero permettere di scegliere al comandante della polizia locale che non vuole affidare a telegram i dati catturati dai lettori di non abilitare questa funzione per i suoi dipendenti. Lasciando però liberi carabinieri e polizia di Stato di orientarsi diversamente.

9. SISTEMI SANZIONATORI STRADALI E DPIA

A parere dell'Autorità di controllo gli strumenti automatici per il controllo del rosso semaforico dovranno essere accompagnati da una valutazione preliminare di impatto privacy. Ed essere identificati con segnaletica ad hoc e un'informativa di secondo livello sulla protezione dei dati. Lo ha evidenziato il Garante per la protezione dei dati con l'innovativo provvedimento del 12 dicembre 2024. I dispositivi omologati per il controllo automatico delle infrazioni stradali sono sempre stati ritenuti esenti dall'obbligo di una valutazione preliminare di impatto privacy, stante la particolare configurazione selettiva dei dati trattati. Con questo severo provvedimento l'Autorità cambia orientamento. Alcuni automobilisti incorsi nel rigore del semaforo rosso hanno presentato reclamo al Garante che ha avviato un'istruttoria che si è conclusa con l'applicazione di una severa misura punitiva a carico del comune di Portici. Oltre a non aver posizionato alcun segnale stradale in prossimità degli impianti e non aver messo a disposizione degli interessati una informativa di secondo livello la negligenza maggiore, a parere del collegio, risulta la mancanza di una valutazione preliminare di impatto privacy. In caso di rischi elevati per gli interessati, specifica infatti il Garante, "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, il titolare del trattamento deve effettuare una valutazione d'impatto sulla protezione dei dati (...). Sul punto il comune ha dichiarato che, all'atto dell'installazione dei dispositivi video in

esame, non ha svolto una valutazione di impatto (...). Si osserva, tuttavia, che il comune era certamente soggetto all'obbligo di redigere una valutazione d'impatto sulla protezione dei dati, considerato che, ai sensi del citato art. 35, par. 3, lett. c), del regolamento, la stessa è sempre richiesta in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico, che consente la raccolta di numerosissimi dati anche inerenti all'ubicazione e alla circolazione degli interessati, circostanza che ricorre nel caso di specie". Con il successivo provvedimento n. 168 del 27 marzo 2025 l'autorità ha però smentito questa impostazione, perlomeno in riferimento ai sistemi ZTL, specificando che "per quanto concerne, invece, il contestato mancato svolgimento della valutazione d'impatto sulla protezione dei dati prima dell'avvio del trattamento dei dati personali (art. 35 del Regolamento), preso atto di quanto dichiarato dal Nuovo Circondario Imolese in corso d'istruttoria in relazione alle peculiarità del sistema di fotocontrollo implementato, [...consistente in] un impianto omologato protetto e isolato, [...] separato e distinto dal sistema di videosorveglianza, il quale ai fini della rilevazione e registrazione delle immagini dei veicoli che accedono all'area Ztl senza permesso autorizzativo, fotografa la targa dei veicoli in transito non censiti in apposita whitelist - contenente l'elenco delle targhe autorizzate ad entrare nell'area ZTL - e non persone o altri veicoli, si dispone, alla luce degli specifici elementi emersi nel caso concreto, l'archiviazione della contestazione della violazione dell'art. 35 del Regolamento".

10. TELECAMERE NEI PE E NELLE CELLE

I gestori dei pubblici esercizi che aderiranno ai protocolli favoriti dal Viminale in materia di videosorveglianza allargata dovranno prestare particolare attenzione alla privacy e alla tutela dei lavoratori. Per evitare sanzioni sarà infatti opportuno procedere con cautela nell'allargamento fai da te dei con i di ripresa delle telecamere e nel possibile coinvolgimento degli istituti di vigilanza e dei servizi di polizia locale. Lo ha evidenziato il decreto del Ministero dell'interno 21 gennaio 2025, pubblicato sulla *GU* n. 20 del 25/01/25. Per una più efficace prevenzione degli atti illegali in prossimità dei pubblici esercizi il Viminale propone la sottoscrizione di accordi locali da formalizzare in conformità alle linee guida allegate al decreto tra il prefetto e le organizzazioni maggiormente rappresentative. I gestori che aderiranno a questi accordi dovranno quindi occuparsi anche di potenziare i propri impianti di videosorveglianza. Secondo indicazioni stringenti non particolarmente chiare lato Gdpr. I sistemi di videosorveglianza privati, specifica innanzitutto il provvedimento, "dovranno essere installati all'esterno del locale pubblico, assicurando la possibilità di riprendere le vie di accesso e le uscite di sicurezza del locale". Questo significa che molti gestori potrebbero essere indotti a riprendere anche strade pubbliche, eventualmente richiedendo il previsto collegamento delle telecamere con istituti di vigilanza o con gli impianti di videosorveglianza comunali. La scelta favorita del decreto di collegare le telecamere private che riprendono strade e piazze con gli impianti di videosorveglianza comunale appare la più lineare, purché le immagini vengano messe a disposizione esclusiva della pubblica amministrazione. In ogni caso restano sullo sfondo questioni fondamentali come la tutela dei lavoratori da regolare preventivamente ai sensi dell'art. 4 dello statuto. Poi sarà opportuno condurre una valutazione di impatto privacy, formare i dipendenti, installare i cartelli, redigere le informative e regolare bene i rapporti con i fornitori. E decidere i tempi di conservazione dei filmati nel rispetto del principio dell'accountability. L'art. 21 del Decreto-Legge 48/2025 introduce e finanzia l'uso della videosorveglianza nei luoghi di privazione della libertà personale (carceri, camere di sicurezza, CPR e strutture sanitarie detentive). La norma mira a garantire trasparenza, prevenire abusi e tutelare sia i detenuti sia gli operatori, consentendo anche l'uso probatorio delle immagini. Il testo lascia irrisolte diverse questioni cruciali: non indica chiaramente quali spazi siano soggetti a sorveglianza, chi possa visionare le immagini, i tempi di conservazione, né quali siano le garanzie per la privacy dei

detenuti.

11. FOTOTRAPPOLE E TUTELA AMBIENTALE

Il dl 116/2025, convertito con modifiche nella legge n. 147/2025, ha introdotto dal 9 agosto 2025 rilevanti modifiche nel contrasto all'abbandono di rifiuti. Anche di piccolissime dimensioni, sia a piedi sia mediante veicoli. Le novità riguardano anche la legittimazione dell'uso delle fototrappole. In ambito stradale, il provvedimento modifica l'art. 15, lett. f-bis, del Codice della Strada, prevedendo una sanzione da 216 a 866 euro per chi getta o deposita rifiuti non pericolosi di piccolissime dimensioni – come fazzoletti, mozziconi di sigaretta o piccoli oggetti – da un veicolo. La nuova formulazione dell'art. 201, comma 5-quater, consente poi l'accertamento di tali violazioni tramite sistemi di videosorveglianza senza obbligo di contestazione immediata, ma subordinatamente a un decreto interministeriale specifico. È previsto l'obbligo di visualizzazione delle immagini entro 24 ore dall'evento. Per l'abbandono pedonale degli stessi rifiuti, l'art. 255, comma 1-bis, del d.lgs. 152/2006 autorizza l'uso della videosorveglianza anche in assenza di contestazione immediata, con sanzione amministrativa comunale compresa tra 80 e 320 euro. Con la legge di conversione del dl 116 è stata poi introdotta un'ulteriore fattispecie sanzionatoria amministrativa ibrida relativa all'abbandono dei rifiuti urbani accanto ai bidoni che, se non costituisce reato, è punita con 1.000 euro di sanzione e l'eventuale fermo amministrativo del veicolo per 1 mese. Il decreto rafforza inoltre il sistema sanzionatorio per le condotte penalmente rilevanti di cui agli artt. 255, 255-bis, 256 e 258 del d.lgs. 152/2006, introducendo la sospensione della patente. Anche queste condotte possono essere documentate dai sistemi di videosorveglianza comunali, ma la norma in questo caso non disciplina le modalità di utilizzo, rimettendo al titolare del trattamento la corretta definizione di finalità e base giuridica. Sul piano della protezione dei dati personali, il provvedimento consolida la base giuridica per l'uso della videosorveglianza nell'accertamento di violazioni amministrative minori, con attenzione al degrado urbano e ai comportamenti incivili. Le finalità dovranno essere ricondotte principalmente alla **sicurezza urbana** o alla **sicurezza stradale**; per gli impianti specializzati nell'accertamento di illeciti penali potrà essere individuata la finalità di **tutela ambientale.**



12. IL RICONOSCIMENTO FACCIALE: L'ULTIMA FRONTIERA

Quasi tutti i comuni hanno impianti di videosorveglianza urbana integrata sempre più potenti in grado di riconoscere le persone e i comportamenti e finalizzati ad assicurare la tutela della sicurezza urbana e della sicurezza pubblica. Ma la raccolta e la conservazione dei dati biometrici ed in particolare il riconoscimento facciale restano ancora un tabù non facilmente superabile senza una base giuridica adeguatamente circoscritta. Lo ha chiarito il Garante con il provvedimento n. 54 del 26 febbraio 2020 (confermato con il parere del 16 aprile 2021). E lo ha ribadito ulteriormente l'art. 9, commi 9, 10, 11 e 12 del dl 139/2021 convertito nella legge 205/2021 in vigore dall'8 dicembre 2021. Pur applicandosi anche agli impianti di videosorveglianza cittadina, specifica il Garante, "la disciplina di cui al d.lgs. n. 51/2018 in ragione dei fini perseguiti dal comune, relativamente alle attribuzioni di polizia giudiziaria della polizia locale o comunque a esigenze di tutela della sicurezza urbana nella componente di prevenzione dei reati, le disposizioni richiamate dall'ente non prevedono specificamente una raccolta di dati biometrici e loro conservazione, nei termini indicati nella richiesta. Tali norme si limitano infatti, in particolare, a consentire l'identificazione dell'indagato e delle persone in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti, a indicare le modalità di attuazione dei principi del codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia, ovvero a legittimare l'installazione di videocamere per fini di tutela della sicurezza urbana e comunque in assenza della specifica previsione normativa della raccolta di dati biometrici, necessaria ai sensi dell'art. 7 d.lgs. n. 51/2018". In buona sostanza, a parere del Garante, l'attività investigativa della polizia giudiziaria con utilizzo di telecamere che consentono il riconoscimento facciale potrà effettuarsi solo in presenza di una espressa previsione normativa. Questa copertura, conclude l'importante parere, "potrebbe eventualmente anche essere contenuta e adeguatamente circoscritta, quanto a presupposti di ammissibilità, nel decreto di prossima adozione di cui all'art. 5, comma 2, del d.lgs. n. 51/2018, così oltretutto uniformando le condizioni per il ricorso a dati biometrici da parte degli enti territoriali, in particolare per le funzioni di polizia giudiziaria riservate alla polizia locale". Con le modifiche introdotte dal dl 139/2021 e con il successivo dl 51/2023, fino al 31 dicembre 2025 è stata di fatto vietata in Italia l'installazione e l'utilizzazione dei sistemi di riconoscimento facciale. Ma con la legge 26/2026 la proroga è slittata al 31

dicembre 2027. Nel frattempo il regolamento Ue 2024/1689, in vigore progressivamente dal 2 agosto 2024, ha ulteriormente disciplinato questa delicata funzionalità sempre al centro dell'attenzione per comprensibili motivi.

13. VIDEOSORVEGLIANZA E TUTELA DEI LAVORATORI

I confini normativi della videosorveglianza nell'ambito dei luoghi di lavoro sono rintracciabili nell'articolo 4 dello Statuto dei Lavoratori, dove si prevede che l'installazione di telecamere e, più in generale, di strumenti dai quali consegua finanche la possibilità di controllo a distanza dell'attività dei prestatori di lavoro, può avvenire unicamente per esigenze di carattere: organizzativo, produttivo, relativo alla sicurezza del lavoro, per la tutela del patrimonio aziendale. All'installazione può procedersi solo previo accordo collettivo stipulato con la rappresentanza sindacale unitaria o aziendale e, ove difettino le rappresentanze sindacali, ovvero non si raggiunga un accordo, gli strumenti di sorveglianza possono essere installati solo dopo aver richiesto l'autorizzazione all'Ispettorato territoriale del Lavoro o, in ipotesi di imprese con unità produttive dislocate negli ambiti di competenza di più ispettorati, alla sede centrale dell'Ispettorato. La Circolare n. 5/2018 è il punto di riferimento operativo: confermando la documentazione che i datori devono presentare per ottenere l'autorizzazione dall'Ispettorato, ribadisce quella già elencata nel comunicato del Ministero del 10 marzo 2017. In linea con tale Circolare, la valutazione delle domande va concentrata sull'effettiva sussistenza delle ragioni che legittimano l'adozione del provvedimento, tenendo presente, in particolare, la finalità per la quale risulta richiesta la singola autorizzazione. In tal modo possono essere autorizzati impieghi di impianti audiovisivi che inquadrano in modo diretto l'operatore, senza dover introdurre condizioni quali, ad esempio, l'angolo di ripresa della telecamera ovvero l'oscuramento del volto del lavoratore, a condizione che sussistano le ragioni giustificatrici del controllo. Con la circolare n. 2572 del 14 aprile 2023 l'Ispettorato ha fornito ulteriori indicazioni operative. Il rispetto delle garanzie di cui all'art. 4 dello statuto dei lavoratori costituisce una condizione di liceità del trattamento, specifica innanzitutto la nota centrale. L'accordo collettivo sindacale costituisce il percorso prioritario e non ha alcun significato l'eventuale consenso del singolo lavoratore.

14. BODYCAM E DRONI A CERTE CONDIZIONI

Per quanto riguarda l'impiego delle bodycam si ritiene opportuno proporre al comando di adottare **un disciplinare** finalizzato a regolare l'ordinario impiego amministrativo di questi dispositivi, **a tutela degli operatori di polizia locale, previa verifica preventiva con le organizzazioni sindacali**, in conformità alle preziose indicazioni che **l'Autorità Garante ha fornito al comune di Torino il 22 marzo 2023. E adottare una DPIA GDPR ad hoc, specifica solo per questi device (come confermato anche con il provvedimento adottato a carico del comune di Pescara il 4 dicembre 2025).** Per quanto riguarda i droni è opportuno fornire adeguata informativa, predisporre cartelli nelle aree sorvolate, e – nei casi di sorveglianza sistematica o su larga scala – valutare con il dpo l'opportunità di una DPIA. L'utilizzo del drone deve rispettare anche le norme aeronautiche (ENAC) e sul tema si è espressa anche la prefettura di Lecce con il provvedimento del 12 febbraio 2026.

Garante privacy al comune di Pescara: no alle body cam della Polizia locale
Rischio di trasferimento dei dati verso paesi extra Ue

Parere negativo del Garante privacy alla valutazione di impatto sulla protezione dei dati personali presentata dal comune di Pescara relativa alle body cam da fornire agli agenti di polizia locale nell'ambito delle attività ausiliarie di pubblica sicurezza e di polizia giudiziaria. Numerose le criticità riscontrate nel sistema nonostante le indicazioni fornite dall'Autorità nel corso di più interlocuzioni. Per quanto riguarda la sicurezza delle soluzioni tecnologiche scelte, il Garante ha accertato che le modifiche inserite nell'ultima valutazione di impatto non forniscono risposta alle richieste di approfondimento tecnico formulate dall'Ufficio. In particolare, posto che il sistema informatico per la gestione dei dati elaborati dalle body cam è fornito da un'azienda statunitense, il comune non ha chiarito se tale scelta abbia tenuto conto di altre soluzioni presenti nel mercato e degli aspetti di protezione dei dati connessi a un trattamento ad elevato rischio come quello effettuato attraverso le body cam.



Il Garante inoltre ha riscontrato l'assenza di misure di sicurezza in grado di escludere che il fornitore del servizio possa accedere in chiaro ai dati trattati dal Comune. Accesso che comporterebbe un trasferimento dei dati verso paesi terzi, in violazione della Direttiva Ue 2016/680 e della normativa privacy.

Il trasferimento di dati personali per scopi di law enforcement, competenza non attribuibile alla società statunitense, è infatti regolato da norme specifiche che impongono rigorose garanzie per trasferimenti transfrontalieri, inclusi accordi vincolanti e un livello adeguato di protezione dei dati nel paese terzo.

Tra le altre criticità anche la presenza di una sim all'interno della body cam su cui non sono stati forniti chiarimenti.

- **base giuridica del trattamento:** nella valutazione d'impatto si legge che le c.d. bodycam "integrano la piattaforma di videosorveglianza fissa comunale, assolvendo gli stessi compiti e basandosi sugli stessi principi normativi, nell'ambito del vigente patto per l'attuazione della sicurezza urbana, anche in funzione anticrimine e antiterrorismo", essendo "tale particolare forma di videosorveglianza, ricondotta all'ambito delle prerogative generali previste per i Comuni dai decreti legge n. 11/2009 e 14/2017". A tal riguardo, occorre far presente a codesto Comune che tali disposizioni normative regolano esclusivamente l'impiego da parte dei Comuni di dispositivi di **videosorveglianza sulla pubblica via, su base continuativa, per finalità di sicurezza urbana, ovvero per la prevenzione e il contrasto dei fenomeni di criminalità diffusa e predatoria**, essendo, peraltro, prevista, quale requisito per il loro impiego, la previa stipula di specifici accordi per l'attuazione della sicurezza urbana con la Prefettura territorialmente competente (v. art. 5, comma 2, lett. a), del d.l. 14/2017). **Tali norme non possono, pertanto, fondare un trattamento di dati personali effettuato mediante bodycam**, che non concretizza una "particolare forma di videosorveglianza". L'impiego delle bodycam, a seconda del contesto, può, invece, essere giustificato, come sopra illustrato, da specifiche esigenze di sicurezza del lavoro, connesse alla tutela dell'incolumità degli operatori di polizia locale in specifiche situazioni di pericolo che giustificano l'attivazione del dispositivo, o da esigenze organizzative, derivanti, ad esempio, dalla necessità di documentare determinate operazioni della Polizia locale (v. art. 4 della l. 300/1970). Spetta a codesto Comune, in qualità di titolare del trattamento, nell'ottica del principio di responsabilizzazione (art. 5, par. 2, del Regolamento), identificare gli specifici casi in cui le bodycam potranno essere impiegate, individuando conseguentemente la corretta base giuridica del trattamento, nei limiti previsti dalla normativa di settore in materia di controllo a distanza dell'attività lavorativa;

15. INTELLIGENZA ARTIFICIALE E VIDEOSORVEGLIANZA

Con l'entrata in vigore del Regolamento UE 2024/1689 (c.d. AI ACT), le amministrazioni comunali che impiegano sistemi di videosorveglianza dotati di intelligenza artificiale (AI) sono tenute ad implementare una serie di misure di adeguamento, assicurando la piena conformità normativa attraverso un processo graduale molto complesso. In particolare, sistemi come il riconoscimento targhe e i software avanzati di analisi video possono essere classificati come "ad alto rischio", in base ai criteri definiti dal regolamento, e richiedono un controllo rigoroso per evitare discriminazioni e utilizzi impropri o sproporzionati. Oltre alla gestione tecnica sarà quindi fondamentale garantire una formazione adeguata e specifica al personale incaricato della gestione e del monitoraggio di tali sistemi. La conformità normativa non si limita a requisiti tecnici, ma include anche l'adozione di protocolli operativi che tutelino i diritti fondamentali e la trasparenza. Occorrerà avviare tempestivamente una mappatura completa dei dispositivi di videosorveglianza attivi, con particolare attenzione ai sistemi dotati di funzionalità di intelligenza artificiale. Questo include la verifica dei software VMS (Video Management System) utilizzati e delle loro capacità, come il riconoscimento automatico delle targhe (ANPR) o l'analisi avanzata delle immagini. È essenziale identificare in particolare i sistemi di intelligenza artificiale "inferenziali", ossia quelli che elaborano dati eterogenei per dedurre informazioni complesse. Successivamente sarà necessario effettuare una revisione completa dei sistemi in uso per identificare eventuali non conformità rispetto al regolamento. I dispositivi non adeguati dovranno essere sostituiti o aggiornati. Parallelamente, andranno implementate misure tecniche e organizzative per garantire la trasparenza e la tracciabilità dei processi decisionali automatizzati. Per i sistemi più critici sarà obbligatoria la redazione di specifiche valutazioni di impatto denominate FRIA. Queste valutazioni dovranno includere un'analisi dettagliata dei potenziali rischi per la privacy, la

sicurezza e i diritti fondamentali, nonché delle misure adottate per mitigarli. Questi adempimenti rappresentano un'opportunità per i comuni di riorganizzare e modernizzare i propri sistemi di videosorveglianza, garantendo al contempo il rispetto dei diritti dei cittadini e una maggiore trasparenza nei processi. La sfida è trasformare un obbligo normativo in un'occasione per migliorare la fiducia pubblica, sfruttando le potenzialità offerte dall'intelligenza artificiale in modo responsabile ed etico.

16. CENNI SULLA CORRETTA PROGETTAZIONE DEGLI IMPIANTI

Per l'installazione di un sistema di videosorveglianza occorre rispettare una serie di norme e regole, non solo le norme in materia di protezione dei dati personali. Per quanto riguarda le fasi di progettazione degli impianti di videosorveglianza urbana, norma tecnica di riferimento è la CEI EN 62676-4, che fornisce prescrizioni per la scelta, la pianificazione, l'installazione e la messa in servizio dei sistemi. Altro aspetto che gli enti dovranno tenere in considerazione è quello riguardante gli eventuali impatti paesaggistici e culturali, con particolare attenzione alle zone e agli edifici sottoposti a vincoli. Un progetto di installazione di telecamere dovrà poi considerare la normativa stradale, evitando interferenze con la segnaletica e la sicurezza della circolazione, con particolare riguardo all'installazione di plinti, pali di sostegno e bracci orizzontali su cui andranno collocate le telecamere. Da un punto di vista puramente tecnico, occorrerà prestare attenzione ai collegamenti elettrici e dovrà essere verificato il limite di carico e di portata dei pali, onde evitare che gli stessi, ad impianto realizzato, si rivelino inadatti a sopportare il peso delle telecamere. Per quanto attiene in particolare ai pali di sostegno e i plinti, sarà necessario dotarsi delle necessarie certificazioni, asseverate da professionisti abilitati. Particolare attenzione andrà poi riservata alla normativa in materia sismica, anche in conformità di quanto imposto dal DPR 380/2001 verificando se le strutture rientrano tra gli interventi privi di rilevanza riguardo alla pubblica incolumità, ovvero tra quegli interventi che, per loro caratteristiche intrinseche e per destinazione d'uso, non costituiscono pericolo per la pubblica incolumità. Ai sensi delle linee guida ministeriali, i plinti di fondazione di pali di illuminazione o di segnaletica non costituiscono pericolo per la pubblica incolumità, al contrario di quanto previsto rispetto ai portali a sbraccio che sostengono le telecamere. Tuttavia, per vedere riconosciuta la non pericolosità, dovrà essere valutata anche la destinazione d'uso. Questo significa che se il palo di sostegno viene installato per l'apposizione di segnaletica e poi diventa un supporto per telecamere, dovrà essere rifatto anche il calcolo strutturale alla luce della nuova destinazione d'uso. La collocazione di sostegni e telecamere, in ogni caso, dovrà avvenire nel rispetto delle norme del codice civile in materia di distanze, altezze e fasce di rispetto delle private abitazioni o proprietà, fatti salvi eventuali accordi di deroga sottoscritti preventivamente con gli interessati. Ultimo aspetto da considerare è quello relativo alle autorizzazioni governative eventualmente necessarie, in base alle tipologie dei mezzi trasmissivi o ponti radio. Per quanto attiene, infine, alla parte di impiantistica e di apparecchiatura interna agli edifici, trova applicazione il DM 37/2008 (*Disposizioni in materia di installazione degli impianti all'interno di edifici*) che individua ulteriori e diverse prescrizioni per committenti, progettisti ed installatori. Nello specifico, l'art. 5, oltre a stabilire l'obbligo di progettazione (realizzazione secondo la regola dell'arte), precisa che il progetto può essere redatto dal responsabile tecnico dell'impresa installatrice, a meno che non si tratti di impianti con particolari caratteristiche, per cui è richiesto l'intervento di un professionista iscritto negli albi professionali (i casi solo elencati al comma 2 dello stesso art. 5). Per quanto riguarda il contenuto dei progetti, il comma 4 dello stesso articolo stabilisce che i progetti dei sistemi da installare devono contenere almeno: gli schemi dell'impianto, i disegni planimetrici e una relazione tecnica sulla consistenza e sulla tipologia dell'installazione dell'impianto stesso, con particolare riguardo alla tipologia e alle caratteristiche dei materiali e componenti da utilizzare e alle misure di prevenzione e di sicurezza da adottare. Se l'impianto subisce

variazioni in corso d'opera, il progetto deve essere integrato con la necessaria documentazione tecnica attestante le varianti. Infine, secondo quanto disposto dall'art. 7 del DM 37/2008, gli installatori devono rilasciare apposita certificazione di conformità. In ultimo, ma non per importanza, è bene ricordare Il Decreto Legislativo 81 del 2008 (*T.U. in materia di tutela della salute e della sicurezza nei luoghi di lavoro*), che individua specifici obblighi in caso di impianti da collocare nei luoghi di lavoro, sia per i committenti, che devono adottare le misure necessarie per salvaguardare i lavoratori, ma anche per i progettisti, tenuti a rispettare i principi generali di prevenzione in materia di salute e sicurezza. La progettazione di un impianto di videosorveglianza comunale richiede infine un'attenta valutazione dei vincoli ambientali, paesaggistici e storico-architettonici previsti dagli strumenti urbanistici locali. In particolare, nelle zone sottoposte a tutela – come i centri storici vincolati ai sensi del Codice dei beni culturali e del paesaggio (D.lgs. 42/2004) – è necessario rispettare le prescrizioni contenute nei regolamenti edilizi, nei piani urbanistici comunali (PRG, PUG) e nei pareri delle Soprintendenze, con particolare riguardo alla collocazione di dispositivi e segnaletica (inclusi i cartelli privacy). L'attività di installazione non può quindi rispondere solo a esigenze contingenti di sicurezza pubblica, ma deve essere preceduta da una fase progettuale integrata, che contempli anche l'impatto visivo e paesaggistico dell'infrastruttura, come richiesto dagli artt. 136 e ss. del D.lgs. 42/2004 e, ove applicabile, dalla disciplina delle aree UNESCO. Inoltre, la progettazione e la realizzazione degli impianti non può essere delegata unicamente alla Polizia Locale, che pur resta responsabile dell'utilizzo operativo e del trattamento dei dati. È indispensabile il coinvolgimento coordinato degli uffici tecnici comunali (per gli aspetti edilizi, impiantistici e viabilistici) e dei CED (per la sicurezza informatica e l'architettura dei dati), in un'ottica multidisciplinare e di conformità normativa.

FASE
B

L'AUDIT PER LA VALUTAZIONE RISCHI



LA VALUTAZIONE DEL CONTESTO E' FONDAMENTALE PER AVVIARE UNA RIORGANIZZAZIONE «DATA GOVERNANCE» DEI SISTEMI DI VIDEOSORVEGLIANZA URBANA. IN PRATICA SI TRATTA DI UN PRIMO CONFRONTO CON TUTTI GLI ATTORI PER CAPIRE I DESIDERATA DELL'ENTE E LO STATO DELL'ARTE

17. LA NIS2 E LA STRETTA SULLA CYBERSECURITY

Con l'entrata in vigore della Direttiva NIS2 (UE 2022/2555) e dlgs 138/2024, gli Enti di maggiori dimensioni e quelli che utilizzano infrastrutture critiche dovranno rivedere profondamente la gestione della videosorveglianza urbana, andando oltre il semplice adeguamento formale. La normativa amplia significativamente gli obblighi di sicurezza,

integrandosi direttamente con il GDPR per la tutela dei dati personali, inclusi quelli biometrici, e con la Direttiva CER per la resilienza fisica e digitale. Gli obblighi prevedono misure tecniche e organizzative proporzionate ai rischi, audit periodici, penetration test e gestione tempestiva degli incidenti con notifiche obbligatorie entro 24 ore. Inoltre, i comuni e gli altri Enti coinvolti dovranno garantire una rigorosa gestione delle catene di fornitura, assicurando che i fornitori rispettino elevati standard di sicurezza informatica. La sinergia tra NIS2 e GDPR richiede che ogni sistema di videosorveglianza sia sottoposto a una valutazione d'impatto privacy (DPIA), coinvolgendo attivamente il DPO fin dalla progettazione del sistema (privacy by design). Parallelamente, la conformità agli standard ISO/IEC 27001 e al framework nazionale per la cybersecurity e la data protection menzionato nella determinazione ACN 14 aprile 2025, diventano un riferimento essenziale per dimostrare l'adeguamento alla NIS2, coprendo aspetti come il controllo degli accessi ai dati, la sicurezza delle credenziali e la gestione dei backup. In concreto, i comuni e gli EELL coinvolti dovranno classificare il proprio sistema di videosorveglianza, aggiornare registri e DPIA, implementare piani strutturati per la gestione degli incidenti e la continuità operativa, rafforzare controlli d'accesso, aggiornare contratti con fornitori e formare il personale su sicurezza e compliance. Questo approccio integrato e strategico segna la fine della semplice installazione di telecamere: i sistemi dovranno diventare resilienti, sicuri e pienamente conformi al quadro normativo europeo, garantendo così maggiore sicurezza e fiducia ai cittadini. In data 20 agosto 2025, infine, ACN ha diramato 20 buone pratiche sulla videosorveglianza sicura applicabili nelle organizzazioni strutturate come gli EELL, in cui l'esposizione di servizi remoti costituisce un rischio critico.

18. LA TUTELA DEI DATI PERSONALI IN GENERALE

Il regolamento Ue 2016/679 e la direttiva 2016/680 hanno ridisegnato la normativa sovranazionale in materia di privacy. Questi provvedimenti hanno reso necessaria l'adozione dei decreti legislativi 10 agosto 2018, n. 101 e 18 maggio 2018, n. 51 che hanno fornito piena integrazione nazionale al pacchetto Ue con una importante riformulazione del D.lgs. 196/2003 (il Codice Privacy italiano). Il regolamento nei suoi novantanove articoli, fornisce numerose conferme dei principi già presenti della disciplina nazionale, ma non manca di introdurre novità di cui si deve tener presente nel trattamento dei dati personali. In prima analisi vi è da dire che, nell'ottica di una maggiore responsabilizzazione - accountability - dei soggetti che effettuano il trattamento delle informazioni, spetta ora al titolare e non già all'Autorità effettuare una valutazione sul bilanciamento tra l'interesse alla gestione dei dati personali e i diritti dell'interessato. In questo senso si intravede il secondo pilastro su cui poggia il nuovo regolamento europeo, ossia il concetto di privacy by design e by default: l'impianto normativo e la responsabilizzazione di tutto l'apparato coinvolto è orientato alla realizzazione di un sistema 'protetto' sin dall'origine, ossia studiato per garantire correttezza del trattamento e quindi la tutela dell'interessato. Anche in materia di informativa e consenso il regolamento apporta novità all'ordinamento nazionale. In particolare, il regolamento disciplina in modo più dettagliato le modalità e i contenuti dell'informativa, in un'ottica di maggiore tutela e trasparenza nei confronti dell'interessato. I contenuti dell'informativa, redatta per iscritto, sono specificati in modo preciso e devono essere facilmente accessibili e comprensibili al destinatario-interessato. Tra i contenuti non dovranno mancare l'indicazione del fondamento giuridico su cui si fonda il trattamento, nonché i riferimenti della neo-introdotta figura del responsabile della protezione dei dati. Nell'art. 12 e seguenti, oltre all'informativa di cui si è già accennato, il regolamento prevede numerosi diritti a favore dell'interessato: il diritto di accesso dell'interessato ai dati personali raccolti dal titolare, il diritto di rettifica o cancellazione dei dati, il diritto di limitazione del

trattamento e il diritto alla portabilità, ossia la possibilità per l'interessato di trasferire i propri dati personali ad un altro interessato. Tuttavia, l'art. 23 del regolamento pone delle eccezioni alla garanzia di tali diritti: infatti la loro portata può essere limitata in presenza di particolari interessi dello Stato, purché ciò rispetti i diritti e le libertà fondamentali e sia necessario e proporzionato. Tra le novità apportate dal regolamento vi è inoltre la valutazione d'impatto sulla protezione dei dati prevista dall'art. 35. Tale incombenza, posta in capo al titolare del trattamento, è prevista per particolari tipologie di raccolta e gestione di dati che possano comportare un elevato rischio per i diritti e le libertà delle persone fisiche interessate (come la videosorveglianza). **La direttiva Ue 2016/680**, attuata in Italia dal decreto legislativo 18 maggio 2018, n. 51, disciplina nello specifico anche i dati personali trattati dalle amministrazioni pubbliche ai fini di prevenzione, accertamento e perseguimento dei reati. La direttiva è strutturata in modo sostanzialmente speculare al regolamento, andando tuttavia a disciplinare un ambito peculiare del trattamento dei dati, sia in funzione delle finalità perseguite, sia in ordine agli interessati coinvolti. Particolare attenzione dovrà essere riposta nella regolamentazione ibrida dei diritti degli interessati, in relazione ai sistemi di videosorveglianza urbana regolati sia ai sensi del Gdpr che del D.lgs. 51/2018. La questione dei diritti di accesso dovrà essere scrupolosamente garantita con una dettagliata procedura interna comunale facendo attenzione a non confondere il diritto d'accesso ai documenti amministrativi, regolato dalla legge 241/1990 e seguenti, rispetto al diritto di accesso al corretto trattamento dei dati degli interessati regolato sia dal Gdpr che dalla direttiva polizia.

19. LE LINEE GUIDA SULLA VIDEOSORVEGLIANZA “GDPR”

Il 29 gennaio 2020 è stata adottata la versione 2.0 delle “Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video” del Comitato europeo per la protezione dei dati – *European Data Protection Board*. In prima battuta, le linee guida affrontano il tema del campo di applicazione del Regolamento UE, escludendo tutti quei casi di riprese video che di fatto non trattano dati personali o che comunque li gestiscono per scopi particolari. Vanno esclusi innanzitutto i trattamenti per “motivi di polizia”, soggetti alla Direttiva UE 2016/680 e al D.lgs. 51/2018; così come devono essere esclusi quelli che – pur riprendendo dati personali altrui – per il loro contenuto e la limitata divulgazione, sono finalizzati a scopi meramente domestici (“esenzione per le famiglie”); devono poi essere esclusi i sistemi che non effettuano riprese (telecamere finte) o le riprese che per qualità o tipologia delle immagini non consentono di risalire ai soggetti ritratti. In seguito, le linee guida affrontano l'aspetto della liceità del trattamento. Questa, da sempre principio cardine della protezione dei dati personali in genere, non può essere solo presunta o supposta, ma deve invece essere sempre documentata in modo concreto e dettagliato, al fine di consentire in qualsiasi momento di legare il trattamento mediante videosorveglianza all'esigenza concreta.

20. LE FAQ DEL GARANTE SULLA VIDEOSORVEGLIANZA “GDPR”

Non servono più autorizzazioni o permessi per attivare impianti di videosorveglianza e l'Autorità andrà consultata solo in casi particolari. Il cuore della riforma sulla tutela dei dati è infatti il principio della responsabilizzazione del titolare del trattamento (*accountability*) che dovrà rendicontare le proprie azioni. Lo hanno evidenziato le FAQ divulgate dal Garante per la protezione dei dati il 3 dicembre 2020. Le risposte non lo specificano ma quando si prende in esame un impianto di videosorveglianza comunale o in genere un sistema di videosorveglianza pubblica, come abbiamo dettagliato in precedenza, occorre prestare particolare attenzione alla disciplina sulla tutela dei dati “uso polizia”, prevista dal D.lgs. 51/2018. In particolare, se l'impianto ha una moderna vocazione interforze in considerazione del fatto che le linee guida n. 3/2019 dell'EDPB non si applicano al trattamento dei dati effettuati dagli impianti di videosorveglianza disciplinati dal D.lgs. 51/2018. Le attività di

ripresa svolte tra i muri domestici per finalità esclusivamente personali esulano dall'applicazione delle regole generali sulla videosorveglianza, specifica il Garante. Come pure l'uso di telecamere false o spente, che ora risultano legittime, oppure quelle che effettuano riprese ad una distanza tale da impedire il riconoscimento delle persone come le telecamere applicate sui droni. Ma attenzione a posizionare telecamere rivolte verso le strade e i palazzi vicini, a parte il rischio di incorrere in reati per interferenza nella vita altrui, le riprese su aree pubbliche e ad uso pubblico sono sempre vietate. Solo i comuni e le forze di polizia possono infatti attivare impianti di videosorveglianza rivolti alle strade pubbliche.

21. I DIRITTI PRIVACY E L'ACCESSO AI FILMATI

Il punto di equilibrio tra privacy, riservatezza ed utilizzo dei dati personali in materia di videosorveglianza secondo la normativa sovranazionale va ricercato anche nella massima trasparenza possibile nel trattamento dei dati personali delle persone fisiche. Il trattato fondamentale dell'Ue, che garantisce un'ampia tutela dei diritti fondamentali del cittadino, deve infatti coesistere con il diritto dell'autorità di estrapolare dati da una ripresa in caso di necessità. Come abbiamo visto, la questione dei diritti di accesso e della massima trasparenza possibile dovrà essere scrupolosamente garantita con una dettagliata procedura interna comunale facendo attenzione innanzitutto a non confondere il diritto d'accesso ai documenti (i filmati), regolato dalla legge 241/1990 e da altre norme speciali, rispetto al diritto di accesso al corretto trattamento dei dati degli interessati regolato sia dal Gdpr che dalla direttiva polizia. Stabilire una procedura significa facilitare la comunicazione tra l'Interessato e il titolare di trattamento, realizzare una simmetria informativa avvisando il cittadino dei diritti di cui gode, delle modalità e dei limiti con cui possono essere esercitati, creare un rapporto di fiducia e aiuto reciproco, oltre che garantire la conformità alle normative. Vi è, quindi, la necessità di stabilire quando e come il cittadino possa conoscere cosa fa il titolare del trattamento con i suoi dati. Con il D.lgs. 51/2018, che ha recepito la direttiva Ue 2016/680, il legislatore assicura una serie di diritti all'interessato esercitabili qualora i dati siano raccolti e trattati nell'ambito di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali. Invece, il Regolamento Ue 2016/679, operante in tutti i casi in cui il trattamento dati è svolto per finalità che esulano da quelle indicate dal D.lgs. 51/2018, assicura all'individuo una lista di diritti che hanno la funzione di bilanciare l'evoluzione tecnologica con la rigorosa applicazione dei principi a tutela del diritto fondamentale degli individui alla protezione dei dati personali.

I DIRITTI DEGLI INTERESSATI

ATTENZIONE A NON
CONFONDERE I **DIRITTI DI
ACCESSO AI FILMATI**
REGOLATI PER LO PIU'
DALLA LEGGE 241/1990 DAI
DIRITTI PRIVACY DEGLI
INTERESSATI REGOLATI DAL
GDPR E DIRETTIVA POLIZIA

22. LE TRE DIVERSE VALUTAZIONI DI IMPATTO PRIVACY

La gestione della videosorveglianza urbana non può più essere sostenuta da una sola valutazione d'impatto generica, perché la pluralità delle finalità perseguite e la diversa natura dei dispositivi utilizzati impongono oggi almeno tre distinte Dpia. L'attività di videosorveglianza comunale, infatti, comporta un trattamento ad elevato rischio per i diritti e le libertà delle persone fisiche e ricade pienamente nell'ambito dell'articolo 35, paragrafo 3, lettera c), del Regolamento (UE) 2016/679 e dell'articolo 23 del Decreto legislativo 18 maggio 2018 n. 51, rendendo obbligatoria una preventiva valutazione d'impatto capace di misurare i rischi del trattamento, le conseguenze sui soggetti coinvolti e le misure tecniche e organizzative necessarie per ridurre il rischio residuo. **La prima Dpia deve riguardare il sistema generale di videosorveglianza finalizzato alla sicurezza urbana** e comprende telecamere fisse, sistemi mobili, fototrappole ambientali e varchi Ocr lettura targhe quando utilizzati per finalità di presidio urbano, controllo del territorio. **Una seconda Dpia autonoma deve invece essere dedicata alla sicurezza stradale**, poiché autovelox, Ztl, photored e sistemi Ocr impiegati per finalità sanzionatorie operano su una base funzionale diversa, legata all'accertamento delle violazioni del codice della strada, con regole differenti in tema di conservazione, accesso e utilizzabilità dei dati. **Una terza valutazione distinta è infine necessaria per le bodycam**, che nella prospettiva più corretta per la Polizia Locale devono essere ricondotte alla tutela del lavoratore e alla protezione dell'operatore durante i servizi più esposti, tenendo conto della particolare invasività di un trattamento mobile, ravvicinato e spesso occasionale. La separazione documentale delle tre Dpia non rappresenta un eccesso burocratico ma una scelta tecnica ormai indispensabile per evitare commistioni tra finalità diverse, rispettare il principio di limitazione della finalità e costruire un sistema realmente coerente sotto il profilo della protezione dei dati.

FASE C

LE CONCRETE MISURE TECNICHE ED ORGANIZZATIVE

Comune di Civitavecchia
Provincia di Roma

PROGETTO DI DEFINIZIONE STRATEGICA E NORMATIVA DELL'IMPIANTO DI VIDEOSORVEGLIANZA COMUNALE CON VARCHI LETTURA TARGHE E NUOVE TECNOLOGIE DEDICATO ALLA SICUREZZA URBANA INTEGRATA

Contrasto dell'attività predatoria e potenziamento della sicurezza locale
LEGGE N. 48/2017
STRATEGIE PER LA VIGILANZA DELLA SICUREZZA URBANA INTEGRATA

Elaborato da: []
Data: 1.8.2018
Foglio: 1 di 1
Autore: Stefano Mancini - Consulente Est. Locali e Forze Di Polizia
Giovanna Turchi - Architetto e Grafico

Validazione: []

DOPO AVER APPROVATO IN GIUNTA IL PROGETTO STRATEGICO OVVERO IL DOCUMENTO PROGRAMMATICO PER LA CORRETTA GESTIONE DEI SISTEMI DI VIDEOSORVEGLIANZA URBANA A VOCAZIONE INTERFORZE OCCORRERA' AVVIARE IL PERCORSO DI REVISIONE ORGANIZZATIVO DEL COMANDO/IN PRATICA:



IN PRATICA UNA VOLTA APPROVATO IL PROGETTO STRATEGICO (O LA RELAZIONE DEL C.TE) IN GIUNTA:

QUALI SONO GLI STEP SUCCESSIVI UNA VOLTA OTTENUTO IL PROGETTO?



1. Il **Progetto** va presentato in **Giunta** per la condivisione degli obiettivi (vedi *modello delibera di Giunta*) e l'attribuzione di una copertura di carattere generale;
2. Il **Progetto** ed il **Patto per la sicurezza** vanno inviati alla **Prefettura** per una prima condivisione di intenti e per aprire gli scenari con un istituto giuridico che stabilizza il rapporto esterno;
3. Il **Regolamento sulla VDS** è l'elemento tecnico che va portato in **Consiglio** e costituisce la base giuridica di trattamento, l'asse portante dei ragionamenti a venire (vedi *modello delibera del Consiglio*).

4. **DPIA** (medio tempone consigliamo di far acquisizione della **bozza di DPIA al protocollo generale** e poi di inviarla al **DPO** insieme al **Progetto** per condividere i processi che si stanno portando a termine. Questo servirà a dimostrare di essere in itinere con l'allineamento normativo, diversamente i tempi sarebbero troppo lunghi. Importante, in questa fase, **condividere i processi**). La DPIA non va assunta con determina, va tenuta agli atti e riservata. Viene infine firmata dal Dirigente.

5. **Ruoli**, nomine e disciplinari operativi
6. **Controllo costante e audit** per la verifica del mantenimento dei requisiti

23. VALUTAZIONE PRIVACY DELLA NECESSITA' E PROPORZIONALITA'

Prima di potenziare, sviluppare o progettare qualsiasi implementazione dell'impianto di videosorveglianza occorrerà riflettere attentamente sul rispetto concreto dei principi fondamentali introdotti dal regolamento europeo in materia di protezione dei dati ovvero il principio di liceità, necessità, proporzionalità, finalità e minimizzazione dei dati. Per evitare

che questi principi restano mere considerazioni teoriche, nella logica dell'accountability, si propone di effettuare anche una periodica *valutazione tecnico - amministrativa* dei progetti e degli impianti che metta in evidenza le seguenti caratteristiche concrete. La liceità del trattamento richiede un'analisi dettagliata della base giuridica che, come abbiamo visto, può essere ricercata in numerose fonti e anche nel regolamento comunale. Particolare attenzione andrà rivolta alla proporzionalità dell'impianto installato alla luce del bilanciamento degli interessi in campo analizzando in particolare il tipo di tecnologia alla quale si ricorre e i dati personali dalla stessa acquisibili mettendoli in correlazione con la finalità del trattamento stesso. Infatti, tale requisito impone di ricorrere alle telecamere solo come misura ultima di controllo, cioè quando altre misure si siano rivelate insufficienti oppure inattuabili. Non è quindi lecito ricorrere all'uso di telecamere solo perché l'impianto è meno costoso rispetto ad altre forme di controllo ma l'analisi tecnica in questione dovrà evidenziare il ruolo strategico e insostituibile svolto da determinate telecamere per il raggiungimento dello scopo prefissato. Infine, andranno analizzati i dati trattati valutando preventivamente che essi siano sempre pertinenti e non eccedenti rispetto alle finalità perseguite. Anche rispetto al criterio della necessità andrà chiaramente esplicitato che, e perché, si ricorra alla videosorveglianza ed in particolare che l'obiettivo perseguito con essa non può essere raggiunto con modalità diverse. Ciò non tanto rispetto all'installazione o meno di telecamere ma piuttosto rispetto alle loro inquadrature, tempistiche e modalità di ripresa evitando usi e tempi sproporzionati od eccessivi. Inoltre, dovrà essere preso in considerazione anche il principio di minimizzazione dei dati, con riferimento non solo alle scelte delle modalità di ripresa, inquadratura e dislocazione delle telecamere, ma soprattutto alla gestione successiva delle varie fasi del trattamento archiviazione conservazione e cancellazione dei dati.

24. LE INFORMATIVE DI PRIMO E SECONDO LIVELLO

La trasparenza del corretto trattamento dei dati personali passa necessariamente anche attraverso una comunicazione efficace e precisa. Il tradizionale cartello stradale con l'icona della telecamera è un elemento molto importante per rendicontare e dimostrare l'accountability, come confermato anche dal provvedimento del Garante n. 531 del 25 settembre 2025 (che ha sanzionato la Provincia autonoma di Bolzano). La nostra raccomandazione è quella di utilizzare un colore diverso dallo sfondo blu per evitare interferenze con il codice stradale ma di riempire di informazioni pertinenti tutto il cartello che poi dovrà necessariamente essere accompagnato da almeno **tre informative di secondo livello raggiungibili facilmente dal cartello**. Almeno una per la **sicurezza urbana**, almeno una per la **sicurezza stradale** e almeno una per la **tutela ambientale**.

	LA REGISTRAZIONE È EFFETTUATA DA: POLIZIA LOCALE COMUNE DI ... PER FINALITÀ: SICUREZZA URBANA STRADALE E AMBIENTALE
	INFORMAZIONI SUL TRATTAMENTO: Videosorveglianza collegata con le centrali delle forze dell'Ordine. Le immagini sono conservate tipicamente per 7 giorni, trascorso tale termine vengono automaticamente cancellate. CONTATTI: Comando di Polizia: TEL. _____ mail _____ Mail DPO: Mail _____
INFORMATIVA DI 2° LIVELLO Per ulteriori informazioni https://www.comune.it GRIGIO EVENTUALE	DIRETTI DELL'INTERESSATO: in qualità di interessato al trattamento puoi rivolgerti al titolare per esercitare i diritti di accesso e cancellazione previsti dal Reg. UE 2016/679 e D.lgs. 51/2018. Per ulteriori e approfonditi dettagli riguardanti questa videosorveglianza puoi sempre consultare l'informativa completa resa disponibile al link sulla sinistra.

Ai sensi
del dl
116/20
25

FASE
D

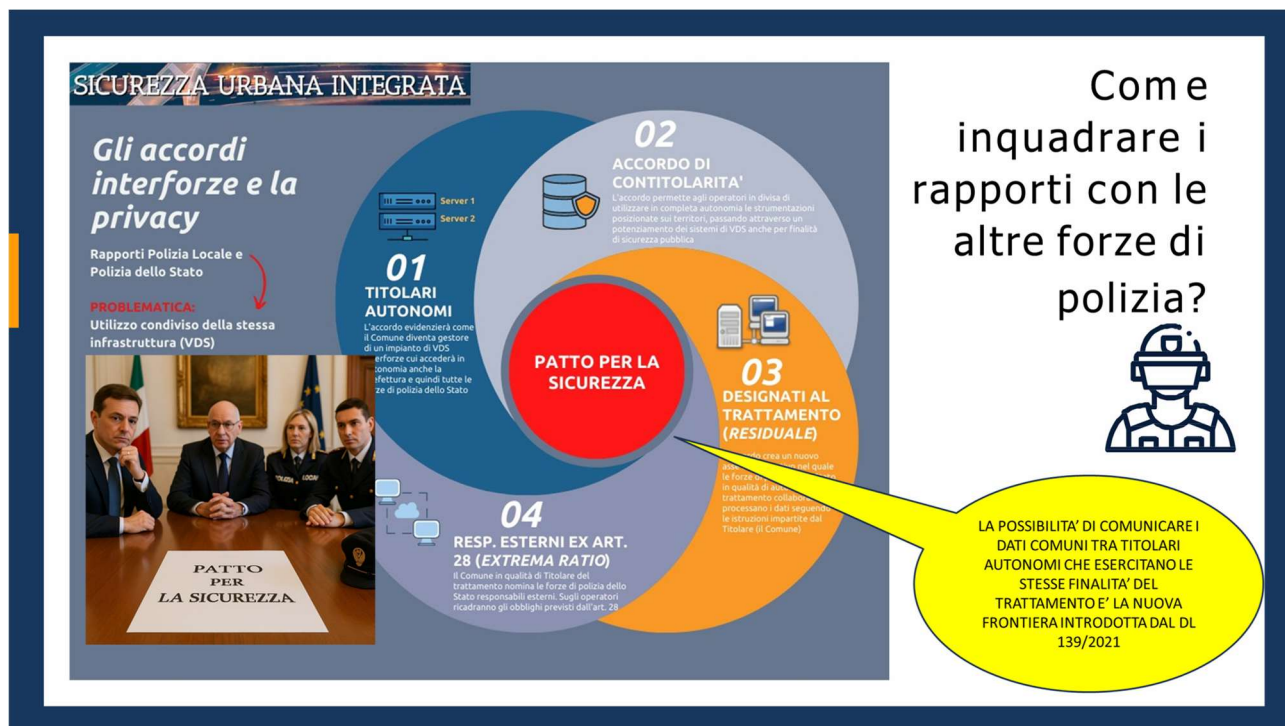
LA TRASPARENZA E LA RENDICONTAZIONE PERIODICA



LE INFORMATIVE SONO IL CAPOSALDO DELLA TRASPARENZA UNITAMENTE ALLA PAGINA WEB SULLA VIDEOSORVEGLIANZA COMUNALE. MA SARA' SOPRATTUTTO LA DPIA LO STRUMENTO PRINCIPE DELL'ACCOUNTABILITY- IL CERTIFICATO CHE FARA' RIPOSARE BENE IL TITOLARE DEL TRATTAMENTO -

25. VERSO UN MODELLO DI PATTO PER LA SICUREZZA NAZIONALE

Con la sottoscrizione dei patti per la sicurezza tra Prefetto e Sindaco prende forma una delle condizioni oggi più rilevanti per attivare correttamente il collegamento interforze tra impianti comunali e sale operative delle Forze di polizia dello Stato. Il tema non è soltanto organizzativo, ma giuridico. Occorre infatti chiarire in modo stabile chi tratta i dati, per quali finalità e dentro quale cornice normativa. Il trend che si sta consolidando è quello della titolarità autonoma. Il Comune resta titolare del trattamento quando raccoglie immagini per finalità amministrative riconducibili alla sicurezza urbana, mentre Polizia di Stato, Arma dei Carabinieri e Guardia di Finanza operano come titolari autonomi quando utilizzano quei medesimi dati per finalità di prevenzione, accertamento e repressione dei reati nel quadro del d.lgs. 51/2018. È dentro questa impostazione che si inserisce la bozza nazionale attesa da tempo e sottoposta all'attenzione dell'Anci in questi mesi destinata a uniformare una materia che finora ha vissuto soprattutto di prassi territoriali molto differenti. Il nuovo schema nazionale di patto tra Prefettura e Comune (divulgato dal Consorzio dei Comuni Trentini il 22 aprile 2026), prova infatti a mettere ordine su accessi, ruoli privacy e collegamenti operativi con le centrali delle Forze di polizia, offrendo finalmente una base comune che potrebbe ridurre molte incertezze applicative. La distinzione è formalmente corretta, ma resta delicata nella pratica. Il dato personale nasce infatti dentro un'infrastruttura comunale progettata prevalentemente in ambito GDPR e può essere immediatamente utilizzato in un diverso perimetro normativo, con finalità tipicamente di polizia. È proprio qui che emergono le principali perplessità. Il rischio è che impianti attivati formalmente per finalità amministrative diventino nella quotidianità strumenti ordinari di controllo generale del territorio, senza che sia ancora pienamente definito il confine giuridico tra sicurezza urbana e sicurezza pubblica. La bozza di testo in circolazione richiama più volte la sicurezza urbana, ma senza valorizzarla fino in fondo come vera base giuridica capace di sostenere una filiera coerente del trattamento. Ma di certo quando questo documento uscirà molte questioni sul tavolo verranno finalmente risolte.



26. ACCORDI INTERFORZE/1: TITOLARITÀ' AUTONOMA

A seguito delle considerazioni espresse anche alla luce delle recenti linee guida europee n. 7/2020 abbiamo alcuni scenari percorribili. La formula "smart" è rappresentata dal paradigma polizia locale e altre forze di polizia dello Stato da considerare e trattare come soggetti esercenti la funzione di titolari autonomi (**indicazione preferita ed in corso di adozione a livello centrale**). Per formalizzare un'attività interforze in questo caso occorrerà regolare un rapporto dove in pratica si specificherà che il comune persegue le finalità di sicurezza urbana con i propri strumenti di videosorveglianza come titolare autonomo. Polizia di Stato e carabinieri dal canto loro perseguono finalità di ordine e sicurezza pubblica e per raggiungere queste finalità potranno ritenere che il mezzo migliore sia l'utilizzo del sistema di videosorveglianza comunale. Per tale motivo, quindi, il Viminale e il Comando generale dell'arma dei carabinieri potranno essere considerati titolari autonomi. Una volta che queste attitudini saranno state formalizzate **in un patto per la sicurezza** si tratterà di disciplinare i rapporti sul trattamento dei dati tra comune e altre forze di polizia con un accordo che metta in evidenza come il comune diventi di fatto il gestore di un impianto di videosorveglianza interforze cui accedono in sicurezza ed autonomia anche polizia e carabinieri, titolari autonomi (ma con finalità convergenti), per lo svolgimento delle proprie attività. Questo accordo "smart" a finalità convergente e complementare evidenzierà in ogni caso anche i limiti e gli obblighi che dovranno essere osservati da tutti gli attori. Le stesse linee guida 7/2020 del Comitato europeo per la protezione dei dati, ai punti 66 e 69, rivalutano l'uso della medesima infrastruttura tecnologica da parte di titolari autonomi, quali comuni e forze di polizia dello Stato, nella direzione già indicata in precedenza dal provvedimento del garante 08/04/2010 n. 1712680.

27. ACCORDI INTERFORZE/2: ACCORDO DI CONTITOLARITÀ'

Alcune prefetture hanno sottoscritto un vero e proprio accordo di contitolarità tra comune e forze di polizia dello Stato. Si tratta delle prime convenzioni sottoscritte a livello nazionale per un utilizzo condiviso dello stesso impianto di videosorveglianza urbana tra forze di polizia locale e dello Stato aggiornata alla riforma europea sulla tutela dei dati personali. La gestione della videosorveglianza urbana integrata a norma di privacy è infatti talmente

complessa da mettere in difficoltà qualunque progettista. Anche perché oltre alle nuove regole sulla tutela dei dati personali tra regolamento Ue 2016/679 e direttiva Ue 2016/680 subentrano le disposizioni sui rapporti interistituzionali dove di fatto i comuni hanno la materiale disponibilità degli impianti mentre le forze di polizia dello Stato hanno le specializzazioni richieste per le attività investigative più riservate. Permettere semplicemente a polizia e carabinieri di utilizzare gli impianti di videosorveglianza in caso di necessità per indagini di polizia giudiziaria è riduttivo. Meglio consentire agli operatori in divisa di utilizzare sempre in completa autonomia tutte le strumentazioni che vengono progressivamente posizionate sui territori. Specialmente se si tratta di tecnologie innovative con analisi video, lettura targhe e intelligenza artificiale. Ma per regolarizzare queste attitudini serve disciplinare i rapporti tra comuni e prefetture mettendo al centro la tutela dei dati personali in un processo che deve essere governato fin dall'inizio seguendo il concetto "privacy by design". Al momento questa strada è stata ritenuta troppo complessa.

28. ACCORDI INTERFORZE/3: NOMINA DI DESIGNATI

La terza ipotesi (**sconsigliata**) per la regolamentazione concreta dei rapporti tra comune e forze di polizia dello Stato è relativa alla nomina di questi ultimi come designati speciali al trattamento ex articolo 2-quaterdecies del codice privacy. Questa ipotesi, di carattere meramente residuale, viene applicata ai soli casi in cui non si possano utilizzare, a causa di una serie di rischi, i regimi previsti dai punti precedenti (contitolarità e titolarità autonoma), in ragione della semplicità informatica degli asset a supporto dei trattamenti (es. assenza di server ridondanti) o per la limitata disponibilità di risorse che garantiscano una corretta gestione dei trattamenti e dei ruoli. Il punto di partenza è la consapevolezza che l'allocazione dei ruoli, nell'ambito delle amministrazioni pubbliche, rappresenta uno degli aspetti più delicati nella complessiva applicazione della disciplina sulla tutela dei dati personali. In questo terzo modello di gestione privacy, quindi, successivamente alla sottoscrizione imprescindibile del patto per la sicurezza, il titolare del trattamento (il comune) nomina le forze di polizia dello Stato designati al trattamento. Questi ultimi, all'interno del nuovo asse organizzativo, rivestiranno la qualifica di autorizzati speciali al trattamento e, a norma dell'art. 2-quaterdecies del codice privacy, collaboreranno e processeranno i dati seguendo le istruzioni impartite dal titolare.

29. ACCORDI INTERFORZE/4: RESPONSABILI ESTERNI

L'ulteriore ipotesi per la regolamentazione concreta dei rapporti tra comune e forze di polizia dello Stato è stata rinverdata da una recente disposizione del Comando generale dell'Arma dei carabinieri che il 22 dicembre 2022 (e successivamente il 1° ottobre 2024) ha specificato che in attesa di diverse indicazioni centrali è possibile formalizzare accordi interforze locali, ai sensi dell'art. 28 del regolamento europeo. Secondo le recenti indicazioni centrali l'Arma dei carabinieri i militari dei comandi territoriali possono partecipare attivamente alla gestione condivisa dei sistemi di videosorveglianza per la sicurezza urbana integrando assumendo il ruolo privacy di responsabile del trattamento ma solo all'esito dello svolgimento positivo di una valutazione di impatto sulla protezione dei dati (dpia) e previa sottoscrizione di un patto per la sicurezza ad hoc.

30. ACCORDI INTERFORZE/5 LA COMUNICAZIONE TRA TITOLARI AUTONOMI

Con la conversione del decreto capienze, il dl 139, la legge n. 205/2021 ha scompaginato l'assetto delle regole generali in materia di corretto trattamento dei dati personali allargando potenzialmente la base giuridica dei trattamenti anche per le azioni di prevenzione dei reati e quindi interferendo, almeno teoricamente, anche con la corretta gestione degli impianti di videosorveglianza urbana. Se lo spirito della riforma è stato da una parte quello di sbloccare

il potenziale informativo ordinario di cui dispone la pubblica amministrazione per agevolare per esempio l'azione di contrasto dell'evasione fiscale e la messa a regime del Pnrr, dall'altra le contraddizioni sono numerose e rischiano di fare precipitare l'interprete in contraddizione con l'assetto sovranazionale del corretto trattamento dei dati personali. Sia dati comuni che particolari ovvero trattati per finalità di prevenzione dei reati. Dall'8 dicembre 2021 la pubblica amministrazione può infatti trattare questi dati basandosi oltre che su una legge o un regolamento anche su un proprio atto amministrativo generale che evidenzi un trattamento necessario per svolgere compiti di pubblico interesse o nell'esercizio di pubblici poteri. Utili suggerimenti operativi, in attesa di eventuali indicazioni centrali, possono riguardare però il potenziamento della base giuridica (con regolamento, delibera e/o determina) per la conservazione allargata fino ad almeno 90-180 giorni dei transiti targhe catturati con gli ocr. Ma anche l'allargamento della base giuridica del trattamento dei dati personali per finalità di polizia ai sensi del novellato art. 5 del dlgs 51/2018. In buona sostanza siccome la tutela della sicurezza stradale urbana è una prerogativa delle amministrazioni comunali sarà possibile allargare la base giuridica del trattamento evidenziando e circoscrivendo le specifiche finalità sempre nel rispetto dei criteri di necessità e proporzionalità aggiungendo anche la possibilità di attivare la comunicazione dei dati tra titolari autonomi che devono raggiungere le medesime finalità (per esempio sicurezza stradale con varchi OCR). Un'altra opportunità messa in campo dalla legge 205/2021 riguarda la possibilità di attivare, ai sensi del nuovo articolo 166/7° del codice privacy, "campagne di comunicazione istituzionale volte alla promozione della consapevolezza del diritto alla protezione dei dati personali" che serviranno a dimostrare la diligenza del titolare del trattamento in caso di ispezioni o controlli.

31. FINALITA' DEI DEVICE AL RESTILING SECONDO L'AUTORITA'

Le finalità perseguite dai sistemi di videosorveglianza comunale, a parere del Garante privacy che si è espresso con la nota inviata a Imola il 18 luglio 2025, devono essere omogenee con puntuali riferimenti alla base giuridica del trattamento. Lo sforzo del titolare dovrà dunque essere orientato a riordinare il più possibile le finalità sotto l'ampia definizione della **sicurezza urbana** che per sua natura può assorbire anche altre finalità gemelle come la protezione civile o il contrasto del degrado. Ma che non può interferire con la sicurezza pubblica senza un patto per la sicurezza ad hoc sindaco – prefetto. Al riguardo, prosegue il documento, "si rammenta che la disciplina di settore consente ai comuni l'impiego di telecamere di videosorveglianza ai soli fini di prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria, previa stipula di un accordo per l'attuazione della sicurezza urbana con la prefettura territorialmente competente". Una seconda finalità ben differenziata può invece essere rinvenuta nella **sicurezza stradale** che attiene ai dispositivi specializzati nel controllo del traffico. Una terza finalità a parere dell'Autorità riguarda la **tutela ambientale** normalmente perseguita con l'uso delle fototrappole. Per quanto riguarda, infine, le finalità **tutela del patrimonio** e tutela della **sicurezza dei lavoratori** non si tratta, tipicamente, di finalità inerenti alle telecamere posizionate sulle vie. In pratica secondo questa recente indicazione centrale possiamo individuare tre finalità tipiche dei sistemi di videosorveglianza urbana posizionati sulle strade. Sicurezza urbana, stradale e ambientale. Indicando nei cartelli queste tre finalità essenziali sarà poi necessario dettagliare i trattamenti nelle procedure e nelle informative di secondo livello. In particolare dopo l'entrata in vigore del dl 116/2025 che ha introdotto nuove finalità eclettiche per il contrasto del degrado che vanno dalla sicurezza stradale alla tutela ambientale. Ma attenzione ai varchi lettura targhe. A parere dell'Autorità se questi device non sono espressamente richiamati nei patti per la sicurezza urbana sottoscritti tra il sindaco e il prefetto, gli stessi non possono essere utilizzati dai comuni per il contrasto della criminalità diffusa e predatoria. In mancanza di indicazioni centrali definitive ed univoche in questo momento è meglio fare un

passo indietro con i sistemi di videosorveglianza comunale dichiarando un uso basilare di queste tecnologie adottando un modello organizzativo che semplifichi le finalità dei trattamenti. Se poi la telecamera inquadrerà un reato la giustizia farà comunque il suo corso.

32. TEMPI DI CONSERVAZIONE DEI FILMATI FACCIAMO CHIAREZZA

Un banale sinistro stradale – nessun ferito, solo due veicoli e un incrocio controllato da telecamere comunali – si è trasformato in una battaglia legale sul diritto di accesso ai filmati e sui tempi di conservazione. Filmati cancellati dopo 5 giorni. L'automobilista coinvolta aveva chiesto di poter visionare le registrazioni per dimostrare che l'altro conducente era passato con il rosso. Il comune, invece di verificare la richiesta, ha risposto mesi dopo che i filmati erano stati automaticamente cancellati dopo cinque giorni, "in applicazione del regolamento comunale". Il TAR Brescia prima e il Consiglio di Stato poi (sent. n. 8472 del 31 ottobre 2025) hanno dato ragione al comune, ribadendo che l'amministrazione non è obbligata a conservare né a recuperare immagini non più esistenti. Formalmente corretto. Operativamente disastroso. Il regolamento comunale, che prevede un periodo massimo di conservazione di cinque giorni, è stato dichiarato conforme al principio di "limitazione della conservazione" del gdpr e all'art. 6 del dl 11/2009, che limita a sette giorni la conservazione per finalità di sicurezza urbana. Ma proprio qui sta il punto: quella norma non vale per tutte le finalità. Quando la videosorveglianza serve a fini stradali, ambientali o di tutela del patrimonio pubblico, non esiste un limite legale rigido (solo per la sicurezza urbana sono previsti per legge 7 giorni). E spetta al titolare del trattamento – cioè al comune stesso – determinare tempi e modalità di conservazione coerenti con lo scopo perseguito. Ma con grande attenzione al principio dell'accountability. **I tempi di conservazione consigliati sono quindi rispettivamente di 7 giorni per finalità di sicurezza urbana, 15 giorni per la tutela ambientale e di 90 giorni per la sicurezza stradale. Ma previa adozione di una delibera/determina ad hoc.**

33. IL CONFRONTO CON GLI ATTORI

Nel corso della videochiamata effettuata il 22 aprile 2026 sono stati esaminati gli aspetti organizzativi generali del sistema di videosorveglianza del comune di Trezzano sul Naviglio. L'impianto è funzionale, avendo beneficiato di aggiornamenti e modifiche nel corso dell'anno precedente. Vi sono circa 60-70 telecamere di contesto gestite tramite software Genetech e 12 varchi lettura targhe muniti di OCR con software Seleca. Il comune dispone di 2 droni impiegati per attività di polizia giudiziaria, che vengono occasionalmente messi a disposizione di altre forze dell'ordine, nonché per il contrasto all'abbandono dei rifiuti sul territorio. Sono in dotazione 8 bodycam, numero destinato ad aumentare sino a 25 unità; prima della loro attivazione è stato sottoscritto nel 2025 un apposito accordo sindacale. Alcuni veicoli della polizia locale sono equipaggiati con dashcam, anch'esse in progressivo aumento. Il comune dispone altresì di telecamere mobili, non assimilabili a fototrappole in senso stretto e dotate di applicativi dedicati, utilizzate esclusivamente per attività di polizia giudiziaria; si tratta di strumentazione di proprietà della polizia locale le cui immagini sono accessibili unicamente al personale del comando. Non sono presenti impianti autovelox fissi; risultano tuttavia attivi 4 impianti per il rilevamento delle infrazioni semaforiche e 3 varchi ZTL. La polizia locale dispone di una centrale operativa unica nella quale confluisce la gestione complessiva del sistema. La gestione tecnica dell'impianto è affidata a due ditte esterne: una incaricata dell'impianto radio e una, denominata TecnoSharing, incaricata della videosorveglianza. Non è stata ancora formalizzata con atto formale la nomina dell'amministratore di sistema, adempimento che dovrà essere espletato contestualmente alla nomina delle medesime ditte quali responsabili esterni al trattamento ai sensi dell'art. 28 del GDPR. Per quanto riguarda i rapporti con le altre forze dell'ordine, i Carabinieri e le altre forze di polizia non sono al momento collegati al sistema di videosorveglianza; le parti

stanno lavorando alla definizione di un accordo che l'ente è disponibile a sottoscrivere esclusivamente a fronte di un'individuazione dei ruoli basata sulla contitolarità. Esiste un precedente accordo del 2021, stipulato con la prefettura in occasione di un finanziamento per i varchi lettura targhe. In tema di tutela dei lavoratori, alcune telecamere esterne agli edifici comunali possono incidentalmente inquadrare dipendenti; è prevista per il prossimo anno l'installazione di alcune telecamere interne in prossimità di locali sensibili quali l'armeria e il locale CED. Tali installazioni interne non sono ancora attive e la loro quantificazione è in corso di definizione; non è stato ancora sottoscritto l'accordo sindacale richiesto dalla normativa, adempimento che verrà comunque completato prima di procedere all'eventuale attivazione. Sul fronte dei rapporti con i privati, al momento non vi sono telecamere di soggetti privati che riprendono il suolo pubblico; l'ente sta tuttavia valutando la possibilità di stipulare convenzioni secondo un modello in cui il privato acquista i dispositivi che vengono poi trasferiti nella disponibilità del comune. Dal punto di vista documentale, il comune è dotato di un regolamento sulla videosorveglianza approvato nel 2022 da riaggiornare alla luce delle novità normative e dell'impianto. Analogamente, la valutazione di impatto privacy (DPIA) esistente, redatta dall'ufficio privacy dell'ente, dovrà essere rifatta in modo da meglio riflettere la realtà attuale. Si segnala inoltre la completa assenza della cartellonistica e dell'informativa di secondo livello, adempimento prioritario che dovrà essere affrontato con la dovuta urgenza. Circa la sicurezza informatica si evidenzia l'importanza di considerare la delicatezza dei dati e delle informazioni presenti sia nella rete informatica che nel sistema di videosorveglianza dell'ente. A tal proposito si renderà opportuna una attività specifica di Cyber Risk Assessment (CRA) che è composta da Vulnerability Assessment Infrastrutturale (VA) e di Penetration Testing (PT). Questi servizi saranno necessari per la verifica della conformità in materia di sicurezza dei dati e più in generale per verificare il grado di sicurezza dei sistemi informatici utilizzati dall'ente in relazione anche al loro collegamento con i sistemi di videosorveglianza. Contemporaneamente al completamento tecnico dell'impianto e previo confronto costante con la prefettura sarà quindi opportuno regolare al meglio tutti gli aspetti organizzativi del comune, Titolare del trattamento, in modo da regolarizzare e rinverdire la formazione del personale, la nomina degli autorizzati e degli altri soggetti ma contemporaneamente aprendo il modello organizzativo alla definitiva collaborazione interistituzionale. In pratica il percorso che si propone di percorrere, meglio esplicitato anche nella scheda riepilogativa allegata in calce, prevede innanzitutto l'approvazione in giunta del presente progetto strategico e il suo trasferimento alla prefettura, per quanto di competenza. Unitamente ad una proposta di un nuovo patto per la sicurezza che richiami anche gli OCR. Con approvazione in Consiglio del nuovo regolamento sulla videosorveglianza.

34. CONCLUSIONI

Per stimolare un processo di corretto adeguamento del crescente sviluppo degli impianti di videosorveglianza urbana alla riforma della tutela dei dati personali e alle esigenze della sicurezza integrata compreso l'AI act si rende necessario prendere atto dell'evoluzione tecnologica e normativa. Il presente studio ha la finalità di avviare e sostenere un percorso condiviso che non può prescindere dalla regolarizzazione della tutela del trattamento dei dati e dalla ricognizione delle esigenze operative e tecnologiche. I confronti con l'Amministrazione comunale hanno evidenziato che gli attori coinvolti in questa operazione hanno una forte consapevolezza dell'importanza di traghettare interventi strutturati di sicurezza urbana integrata. È attualmente presente un parco tecnologico in corso di costante aggiornamento. Ora si tratta di procedere a perfezionare tutti gli atti e le attività organizzative necessarie al fine di completare l'attività anche con una necessaria valutazione di impatto privacy (dpi). Dopo aver approvato il presente documento in Giunta sarà opportuno trasmettere il progetto in Prefettura, portare in Consiglio Comunale il nuovo

regolamento sulla videosorveglianza e procedere successivamente con la formazione degli operatori, gli eventuali ulteriori accordi sindacali, le nomine e con tutte le attività necessarie alla redazione di una robusta valutazione di impatto privacy.

Faenza, 1 giugno 2026

Allegati:

- 1. Traccia del patto per la sicurezza divulgato il 22 aprile 2026 in Trentino**
- 2. Schema regolamento aggiornato sulla videosorveglianza**
- 3. Scheda passi successivi alla redazione del presente progetto**



STEFANO MANZELLI
Via Comandini, 4
48018 FAENZA (RA)
C.F. MNZ SFN 64T01 D458L
P.IVA 02569530393