



**COMUNE DI
TREZZANO SUL NAVIGLIO**
CITTA' METROPOLITANA DI MILANO
Via IV Novembre, 20090

**VERBALE DI DELIBERAZIONE DELLA
GIUNTA COMUNALE**

N. 166 del 09/09/2026

ORIGINALE

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

L'anno **duemilaventisei** addì **nove** del mese di **settembre** alle ore **10:00** nella Residenza Comunale, convocata nei modi di legge, si è legalmente riunita la Giunta Comunale.

MORANDI GIUSEPPE LUIGI	SINDACO	Presente
PULEO ANTONINO	VICE SINDACO	Presente
DI BISCEGLIE MATTIA	ASSESSORE	Presente
FERRANTE PAOLA	ASSESSORE	Assente
PIRANI LUISELLA	ASSESSORE	Presente
MENTO SALVATORE	ASSESSORE	Presente

Presenti n. 5

Assenti n. 1

Partecipa il VICESEGRETARIO COMUNALE FESTA ANTONIO .

Il Sig. MORANDI GIUSEPPE LUIGI assume la presidenza, riconosciuta valida l'adunanza, dichiara aperta la seduta e dà avvio alla discussione sull'oggetto all'ordine del giorno.

Si dà atto che nessuno degli assessori presenti ha dichiarato la propria incompatibilità con l'oggetto della presente deliberazione, ai sensi dell'art. 78 comma 2 del D.Lgs. 267/2000.

LA GIUNTA COMUNALE

VISTO lo Statuto comunale vigente;

VISTO il Regolamento comunale di Organizzazione;

VISTO il Regolamento comunale di Contabilità;

VISTA la deliberazione del Consiglio comunale n. 92 del 26/09/2025 con la quale è stato approvato il Documento Unico di Programmazione (D.U.P.) per il triennio 2026/2028;

VISTA la deliberazione del Consiglio comunale n. 1 del 07/01/2026 immediatamente eseguibile avente ad oggetto "Approvazione Nota di aggiornamento del Documento Unico di Programmazione (D.U.P.) per il triennio 2026/2028 e relativi adempimenti";

VISTA la deliberazione del Consiglio comunale n. 2 del 07/01/2026 immediatamente eseguibile avente ad oggetto: "Approvazione del Bilancio di previsione 2026/2028 e relativi adempimenti";

RICHIAMATA la deliberazione del Consiglio comunale n. 18 del 24/02/2026 avente ad oggetto: "Manovra di Bilancio 2026/2028: riapprovazione Nota di aggiornamento DUP 2026/2028, Bilancio di previsione 2026/2028 e relativi adempimenti";

RICHIAMATA altresì la deliberazione della Giunta comunale n. 39 del 04/03/2026 avente ad oggetto: "Approvazione Piano Esecutivo di Gestione (P.E.G.) per il triennio 2026/2028 a seguito di riapprovazione manovra di Bilancio";

RICHIAMATA la deliberazione della Giunta comunale n. 73 del 15.04.2026 con la quale è stato approvato il P.I.A.O. 2026/2028 (documento nel quale è confluito il Piano Triennale di Prevenzione della Corruzione e della Trasparenza);

VISTO l'art. 48, comma 1 del D.Lgs. 267/2000;

Visto l'art. 5 del decreto-legge n. 14/2017, convertito con modificazioni dalla legge 18 aprile 2017, n. 48, recante "*Disposizioni urgenti in materia di sicurezza delle città*" e i relativi provvedimenti attuativi, nonché l'art. 6 del dl 23 febbraio 2009, n. 11, recante misure urgenti in materia di sicurezza pubblica;

Visto il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;

Vista la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati;

Visto l'articolo 15 della legge 241 del 1990 - Accordi fra pubbliche amministrazioni, che consente alle amministrazioni pubbliche di concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune;

Visto il nuovo articolo 2-ter del Codice Privacy così come modificato dalla legge 205 del 2021 di conversione del d. lgs. 139/2021 (Decreto capienze);

Considerata la necessità di potenziare gli impianti di videosorveglianza comunale con predisposizione degli stessi ad un corretto uso anche condiviso con le altre forze di polizia nel pieno rispetto della tutela dei dati personali e delle diverse

prerogative della polizia locale e di quelli della polizia dello Stato;

Vista la traccia di regolamento comunale per la videosorveglianza;

Visto il lavoro di definizione strategica e normativa dell'impianto di videosorveglianza intercomunale con varchi lettura targhe e nuove tecnologie dedicato alla sicurezza urbana integrata, allegato alla presente deliberazione, redatto dal gruppo di ricerca www.sicurezzaurbanaintegrata.it il 01/06/2026;

Ritenuto necessario proporre alla prefettura di sottoscrivere il modello di patto per la sicurezza, allegato alla presente e redatto ai sensi delle Linee generali delle politiche per la sicurezza integrata, adottate in sede di Conferenza Unificata il 24 gennaio 2018, e delle Linee Guida per l'attuazione della Sicurezza Urbana, approvate dalla Conferenza Stato città ed autonomie locali in data 26 luglio 2018, avente come scopo il potenziamento dell'attività interforze e il potenziamento degli impianti di videosorveglianza urbana nell'ottica di una sicurezza urbana integrata, prevedendo anche la possibile partecipazione dei privati;

Ritenuto necessario conseguentemente adottare un accordo di contitolarità tra il Comune di Trezzano sul Naviglio e le altre forze di polizia per permettere l'uso integrale di tutte le dotazioni a tutti gli operatori, ovvero, in alternativa, un accordo di altra natura;

Dato atto che, ai sensi dell'art. 49 del Decreto Legislativo 18 agosto 2000 n. 267, sono stati acquisiti ed allegati alla presente deliberazione, di cui costituiscono parte integrante e sostanziale, i pareri in ordine alla regolarità tecnica e contabile espressi dal Responsabile di Settore competente;

Ad unanimità di voti favorevoli espressi nei modi di legge,

D E L I B E R A

Di approvare il progetto di definizione strategica e normativa allegato alla presente deliberazione;

Di approvare lo schema di regolamento per la videosorveglianza come base giuridica per la redazione del nuovo regolamento che dovrà basarsi sul progetto strategico e l'aggiornamento normativo al fine di poter successivamente inoltrarlo al Consiglio comunale al fine di proporre la sua approvazione;

Di approvare lo schema di proposta di patto per la sicurezza allegato alla presente deliberazione;

Di autorizzare il Sindaco a sottoscrivere il patto per la sicurezza con il Prefetto di Milano;

Di autorizzare il Sindaco a sottoscrivere l'accordo di contitolarità per la gestione della videosorveglianza con le altre forze di polizia o altro accordo simile;

Successivamente, ad unanimità di voti, resi nelle forme di legge,

D E L I B E R A

Di dichiarare il presente atto immediatamente eseguibile ai sensi dell'art. 134 comma 4° del D.Lgs. 267/00, con successiva e separata votazione unanime, stante l'urgenza di provvedere in merito.

Letto, approvato e sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.

II SINDACO
MORANDI GIUSEPPE LUIGI

II VICESEGRETARIO COMUNALE
FESTA ANTONIO

PATTO PER LA SICUREZZA URBANA FINALIZZATO
ALLA GESTIONE INTEGRATA DEL SISTEMA
COMUNALE DI VIDEOSORVEGLIANZA TRA

IL COMUNE DI TREZZANO SUL NAVIGLIO

E

LA QUESTURA DI MILANO

IL COMANDO PROVINCIALE DEI CARABINIERI

IL COMANDO PROVINCIALE DELLA
GUARDIA DI FINANZA

Il Sindaco di Trezzano sul Naviglio, il Questore di Milano, il Comandante Provinciale dell'Arma dei Carabinieri di Milano ed il Comandante Provinciale della Guardia di Finanza.

CONSIDERATO

che, per garantire adeguati livelli di sicurezza urbana, le Forze di Polizia ad ordinamento nazionale e locale, a diverso titolo competenti, sono chiamati, nel rispetto di specifiche attribuzioni, a sviluppare in forma coordinata interventi volti alla riqualificazione e al recupero di aree urbane, all'eliminazione dei fattori di marginalità ed esclusione sociale, alla promozione della cultura della legalità e della coesione sociale, nonché alla prevenzione della criminalità, in particolare di quella predatoria;

che, l'esperienza in questo ambito, il ricorso ai sistemi di videosorveglianza da parte dei predetti soggetti istituzionali costituisce uno strumento in grado di contribuire ad innalzare il gradiente della sicurezza urbana, sia attraverso l'installazione di nuovi apparati, sia favorendo l'aggiornamento di quelli già esistenti;

che la Corte Costituzionale, nella sentenza 12 novembre 2020 n. 236, ha ribadito che la prevenzione dei reati e il controllo del territorio costituiscono il nucleo centrale della funzione di pubblica sicurezza, di competenza esclusiva dello Stato, a mente dell'articolo 117, secondo comma, lettera h), della Costituzione e demandata, dalla Legge 01 aprile 1981 n. 121, alle Autorità di Pubblica Sicurezza ed alle Forze di Polizia;

che, come previsto dalle linee generali delle politiche pubbliche per la promozione della sicurezza integrata, adottate con accordo sancito in sede di Conferenza Unificata in data 24 gennaio 2018, ai sensi dell'articolo 2, comma 1, del Decreto Legge 20 febbraio 2017, n. 14, convertito con modificazioni dalla Legge 18 aprile 2017, n. 48, la collaborazione delle Forze di Polizia e la Polizia Locale, contempla anche l'utilizzo in comune di sistemi di sicurezza tecnologica finalizzati al controllo delle aree e delle attività soggette a rischio;

che, come sottolineato dall'Accordo in merito alle Linee Guida per l'attuazione della sicurezza urbana tra la Conferenza Stato-Città ed Autonomie locali e il Ministero dell'Interno, stipulato il 26 luglio 2018, ai sensi dell'articolo 5, comma 1, del Decreto-Legge 20 febbraio 2017, n. 14, convertito con modificazioni dalla Legge 18 aprile 2017, n. 48, la gestione coordinata dei sistemi di videosorveglianza installati dai Comuni può costituire una delle attuazioni concrete della cooperazione tra le Polizie Locali e le Forze di Polizia dislocate sul territorio;

che tra gli obiettivi per l'attuazione della sicurezza urbana, indicati nelle succitate linee guida, vi è, inoltre, la promozione e la tutela della legalità, anche mediante mirate iniziative di dissuasione di ogni forma di condotta illecita, concernente, in particolare, il contrasto alla vendita di beni contraffatti e all'abusivismo commerciale correlato alle non corrette occupazioni del suolo pubblico;

che il Comune di Trezzano sul Naviglio ha progettato e realizzato un sistema di videosorveglianza che intende impiegare al fine di contribuire ad innalzare il livello della sicurezza urbana, contribuendo alla prevenzione e al contrasto dei fenomeni criminali, in particolare di quelli di tipo predatorio;

che il trattamento dei dati personali effettuato dal Comune di Trezzano sul Naviglio mediante il predetto sistema di videosorveglianza, essendo finalizzato alla tutela della sicurezza urbana, è disciplinato dal Regolamento (UE) 27 aprile 2016, n. 679, recante «Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)»;

che il Comune di Trezzano sul Naviglio ha altresì progettato e realizzato un sistema di lettura targhe per il controllo stradale, utilizzato per il controllo in tempo reale di veicoli rubati (tramite connessione alla rete SCNTT), assicurazione scaduta o revisione mancante (tramite "Il Portale dell'Automobilista") e che, tramite algoritmi di ricerca, consente di utilizzare le immagini raccolte per la ricerca di veicoli a fini statistici o di polizia giudiziaria;

che il trattamento dei dati personali effettuato dal Comune di Trezzano sul Naviglio mediante il predetto sistema di lettura targhe, è disciplinato dal citato regolamento (UE) 27 aprile 2016, n. 679;

che i dati raccolti con il sistema di videosorveglianza e con il sistema di lettura targhe, sono accessibili al Servizio di Polizia Locale del Comune di Trezzano sul Naviglio per essere ulteriormente utilizzati al fine di adempiere agli obblighi correlati all'assolvimento delle funzioni di polizia giudiziaria attribuite dalla Legge 7 marzo 1986, n. 65. Tale ulteriore trattamento di dati personali per finalità di indagine penale è disciplinato dal Decreto legislativo 18 maggio 2018, n. 51;

che, inoltre, è intendimento del Comune di Trezzano sul Naviglio attivare un collegamento con le Sale o Centrali Operative degli Uffici e dei Comandi delle Forze di Polizia di cui all'articolo 16 della Legge 01 aprile 1981, n. 121, per consentire la visione delle immagini in tempo reale ed in differita, mediante l'accesso al sistema di videosorveglianza predetto;

che, pertanto, è intendimento del Comune di Trezzano sul Naviglio attivare un collegamento con la Questura di Milano per consentire la comunicazione dei dati raccolti dal proprio sistema di lettura targhe al Centro elettronico nazionale della Polizia di Stato (CEN), ai fini dell'elaborazione informatica da parte del "Sistema di controllo nazionale targhe e transiti" (SCNTT);

che il Comitato Provinciale per l'Ordine e la Sicurezza, nella seduta del _____, ha espresso il proprio parere favorevole sul testo del presente protocollo, anche per quanto concerne la necessità di prevedere, alla luce di quanto stabilito dalle vigenti norme in materia, la titolarità autonoma dei trattamenti dei dati personali acquisiti attraverso il sistema di videosorveglianza, in ragione delle differenti finalità per le quali i medesimi trattamenti possono essere effettuati;

VISTI

- il Regolamento (UE) 27 aprile 2016, n. 679, recante «Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»;
- il Regio Decreto 18 giugno 1931, n. 773, recante «Testo unico delle Leggi di Pubblica Sicurezza»;
- la Legge 01 aprile 1981, n. 121, «Nuovo ordinamento dell'Amministrazione della Pubblica Sicurezza»;
- in particolare, l'articolo 24 della predetta Legge n. 121 del 1981 che, nell'individuare i compiti istituzionali della Polizia di Stato, prevede, tra l'altro, che essa assicuri la tutela dell'ordine e della sicurezza pubblica, nonché le attività di prevenzione e repressione dei reati;
- la Legge 7 marzo 1986, n. 65, recante «Legge-quadro sull'ordinamento della Polizia Municipale»;
- l'articolo 159, comma 2, del Decreto Legislativo 31 marzo 1998, n. 112, secondo cui le funzioni relative all'ordine pubblico e alla sicurezza pubblica concernono le misure preventive e repressive dirette al mantenimento dell'ordine pubblico, come il complesso dei beni giuridici fondamentali e degli interessi pubblici primari sui quali si regge l'ordinata e civile convivenza nella comunità nazionale, nonché alla sicurezza delle Istituzioni, dei cittadini e dei loro beni;
- il Decreto Legislativo 19 marzo 2001, n. 68, recante «Adeguamento dei compiti del Corpo della Guardia di Finanza, a norma dell'articolo 4 della Legge 31 marzo 2000, n. 78» e, in particolare, l'art. 2, comma 2, lettera I), che attribuisce alla Guardia di Finanza compiti di prevenzione, ricerca e repressione delle violazioni, tra l'altro, in materia di brevetti, marchi e altri diritti di privativa industriale;
- il Decreto Legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali, recante disposizioni l'adeguamento dell'ordinamento nazionale al regolamento UE n. 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE»;

- in particolare, l'art. 2-ter, comma 1, del predetto Decreto Legislativo n. 196 del 2003, secondo cui la base giuridica per i trattamenti di dati personali è costituita da una norma di legge o di regolamento ovvero da atti amministrativi generali;
- il Decreto Legge 23 maggio 2008, n. 92, convertito dalla Legge 24 luglio 2008, n. 125, recante «Misure urgenti in materia di sicurezza pubblica», relativo alla collaborazione della Polizia Locale Comunale e Provinciale nell'ambito dei piani coordinati di controllo del territorio;
- il Decreto Legge 23 febbraio 2009, n. 11, convertito, con modificazioni, dalla Legge 23 aprile 2009, n. 38, recante «Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori» e in particolare l'articolo 6, commi 7 e 8, che autorizza i Comuni a installare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana, stabilendo in sette giorni il termine massimo di conservazione dei dati personali acquisiti attraverso i predetti sistemi;
- l'articolo 159 del Decreto Legislativo 15 marzo 2010 n. 66 che, nell'individuare i compiti di istituto dell'Arma dei Carabinieri, quale Forza Armata a competenza generale e in servizio permanente di pubblica sicurezza prevede, tra l'altro, che essa assicuri il mantenimento dell'ordine pubblico, della sicurezza dei cittadini, della loro incolumità e della tutela della proprietà;
- il Decreto-Legge 20 febbraio 2017, n. 14, convertito, con modificazioni, dalla Legge 18 aprile 2017, n. 48, recante «Disposizioni urgenti in materia di sicurezza delle città»;
- in particolare, l'articolo 1 del predetto Decreto Legge n. 14 del 2017, che definisce la sicurezza integrata come l'insieme degli interventi assicurati dallo Stato, dalle Regioni, dalle Province autonome di Trento e Bolzano e dagli enti locali, nonché dagli altri soggetti istituzionali, al fine di concorrere, ciascuno nell'ambito delle proprie competenze e responsabilità, alla promozione e all'attuazione di un sistema unitario e integrato di sicurezza per il benessere delle comunità territoriali;
- altresì, l'articolo 2 del medesimo Decreto Legge n. 14 del 2017, il quale prevede che le linee generali delle politiche pubbliche per la promozione della sicurezza integrata sono adottate, su proposta del Ministro dell'interno, con accordo sancito in sede di Conferenza unificata, precisando che tali linee generali riguardano, tra l'altro, la collaborazione tra le Forze di Polizia e le Polizie Locali nei settori dello scambio informativo, per gli aspetti di interesse nell'ambito delle rispettive attribuzioni istituzionali, dell'interconnessione, a livello territoriale, delle Sale Operative e della regolamentazione dell'utilizzo in comune di sistemi di sicurezza tecnologica finalizzati al controllo delle aree e delle attività soggette a rischio;
- inoltre, l'articolo 4 del ripetuto Decreto Legge n. 14 del 2017 secondo cui la sicurezza urbana è il bene pubblico che afferisce alla vivibilità e al decoro della città, da perseguire con interventi riguardanti, tra l'altro, la prevenzione della criminalità, in particolare di tipo predatorio, ed alla cui realizzazione concorrono prioritariamente, anche con interventi integrati, lo Stato, le Regioni, le Province autonome di Trento e Bolzano, e gli enti locali, nel rispetto delle rispettive competenze e funzioni;
- infine, l'articolo 5 del citato Decreto Legge n. 14 del 2017, secondo cui gli interventi per la sicurezza urbana possono essere individuati, in coerenza sia con le linee generali delle politiche pubbliche per la promozione della sicurezza integrata, sia con le linee guida approvate, su proposte del Ministro dell'Interno, con accordo sancito in sede di Conferenza Stato-Città e Autonomie Locali, attraverso appositi patti sottoscritti tra il Prefetto e il Sindaco, concernenti, tra l'altro, la prevenzione e il contrasto dei fenomeni di criminalità diffusa e predatoria, la tutela della legalità, nonché la promozione del rispetto del decoro urbano;
- il Decreto legislativo 18 maggio 2018, n. 51, recante «Attuazione della direttiva UE 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio»;
- il Decreto legislativo 19 agosto 2016, n. 177, recante «Disposizioni in materia di razionalizzazione delle funzioni di polizia e assorbimento del Corpo Forestale dello Stato, ai sensi dell'articolo 8, comma 1, lettera a), della Legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche»;

- il Decreto del Presidente della Repubblica 15 gennaio 2018, n. 15, recante «Regolamento a norma dell'articolo 57 del Decreto Legislativo 30 giugno 2003, n. 196, recante l'individuazione delle 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»;
- il Decreto Ministeriale del 24 maggio 2017, recante l'individuazione dei trattamenti di dati personali effettuati dal Centro Elaborazione Dati del Dipartimento della Pubblica Sicurezza o da Forze di Polizia sui dati destinati a confluirci, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di Legge o di regolamento, effettuati con strumenti elettronici e i relativi titolari, in attuazione dell'articolo 53, comma 3, del Decreto Legislativo 30 giugno 2003, n. 196 e, in particolare, l'allegata scheda numero 15, concernente i trattamenti di dati personali effettuati attraverso i sistemi di videosorveglianza;
- il Decreto del Ministro dell'Interno in data 15 agosto 2017, recante "Direttiva sui comparti di specialità delle Forze di Polizia e sulla razionalizzazione dei presidi di polizia";
- le "Linee generali delle politiche pubbliche per la sicurezza integrata" adottate, ai sensi dell'art. 2 del Decreto-Legge n. 14 del 2017, con accordo sancito in sede di Conferenza unificata del 24 gennaio 2018;
- in particolare, il paragrafo 5 delle predette linee generali il quale, nel confermare che tra gli obiettivi degli interventi di sicurezza integrata vi è anche la realizzazione di una razionale copertura del territorio, in grado di assicurare il "videocontrollo" dei luoghi a rischio di degrado o di criminalità diffusa, precisa che l'utilizzazione in comune dei sistemi di videosorveglianza, da parte delle Forze di Polizia e delle Polizie Locali, deve avvenire in ossequio al principio del "rispetto delle rispettive competenze", tenendo conto che l'accesso ai sistemi da parte delle Polizie Locali avviene per l'esercizio dei compiti di sicurezza urbana e per lo svolgimento degli altri compiti istituzionali ad esse demandati, mentre i sistemi di videosorveglianza attivati dalle Forze di Polizia rispondono alle finalità di prevenzione generale dei reati e di salvaguardia della sicurezza pubblica di esclusiva competenza statale;
- le Linee guida per l'attuazione della sicurezza urbana, ai sensi dell'articolo 5, comma 1, del Decreto Legge 20 febbraio 2017, n. 14, adottate con accordo sancito in sede di Conferenza Stato-città ed Autonomie locali nella seduta del 26 aprile 2018, le quali ribadiscono che i patti sottoscritti tra il Prefetto e il Sindaco possono prevedere, tra gli altri interventi di sicurezza urbana, anche la realizzazione e l'innalzamento del livello tecnologico degli impianti di videosorveglianza del territorio, potendo accedere, a tal fine, anche ad appositi fonti di finanziamento previste da norme di Legge;
- le Linee guida n. 3/2019 sul trattamento dei dati personali attraverso dispositivi video adottate dal Comitato per la protezione dei dati il 29 gennaio 2020;
- il provvedimento n. 1712680 in materia di videosorveglianza adottato dal Garante per la protezione dei dati personali in data 8 aprile 2010;
- la direttiva del Ministro dell'Interno, concernente le nuove linee strategiche per il controllo coordinato del territorio, n. 11001/110 (23) datata 30 aprile 2015;
- il Protocollo d'Intesa per la videosorveglianza sottoscritto in data __/__/____ tra il Sindaco ed il Prefetto di Milano per la realizzazione di un sistema integrato di controllo del territorio attraverso la mappatura, la georeferenziazione, l'implementazione e la razionalizzazione dei sistemi di videosorveglianza e lettura targhe presenti sul territorio provinciale da riconnettere con le Sale/Centrali operative delle Forze dell'Ordine, per consentire, in tempo reale, la visione ed il prelievo delle immagini, sia a scopi preventivi che di contrasto alle fenomenologie criminose;
- la circolare del Dipartimento della Pubblica Sicurezza - Direzione Centrale per gli Affari Generali della Polizia di Stato n.0001065 del 12 gennaio 2018 «Realizzazione dei sistemi di lettura targhe ed integrazione al Sistema di Controllo Nazionale Targhe e Transiti (SCNTT) - Linee di indirizzo»;
- la delibera n. __ del __/__/____ con la quale il Consiglio Comunale di Trezzano sul Naviglio ha approvato il regolamento per la disciplina del sistema di videosorveglianza;

CONVENGONO QUANTO SEGUE

Capo I **Disposizioni generali**

Art. 1

Ambito di applicazione

1. Con il presente atto, il Sindaco di Trezzano sul Naviglio (in qualità di rappresentante legale del Comune di Trezzano sul Naviglio), ai sensi della normativa richiamata in premessa, stipula con il Questore di Milano, il Comandante Provinciale dei Carabinieri ed il Comandante Provinciale della Guardia di Finanza, un accordo attuativo del Patto per la sicurezza Urbana, definendo, nel rispetto delle vigenti norme in materia di protezione dei dati personali, le modalità di gestione, e utilizzazione del sistema di videosorveglianza e lettura targhe installato dal Comune di Trezzano sul Naviglio per garantire più elevati livelli di sicurezza urbana nel proprio territorio.
2. Il presente accordo definisce altresì i termini secondo i quali i dati raccolti dal sistema di videosorveglianza sono resi disponibili dal Comune di Trezzano sul Naviglio alla Questura di Milano, al Comando Provinciale dei Carabinieri di Milano ed al Comando Provinciale della Guardia di Finanza di Milano, per l'espletamento dei compiti di prevenzione e repressione dei reati e per la tutela dell'ordine pubblico. Definisce ancora i termini secondo i quali i dati raccolti dal predetto sistema di lettura targhe sono comunicati al Centro elettronico nazionale della Polizia di Stato (CEN), ai fini dell'elaborazione informatica da parte del "Sistema di controllo nazionale targhe e transiti" (SCNTT).
3. Le premesse di cui al preambolo fanno parte integrante del presente patto.

Art. 2

Definizioni

1. Ai fini del presente patto, si intende per:
 - a) "*Codice della strada*", il nuovo Codice della Strada di cui al Decreto Legislativo 30 aprile 1992, n. 285;
 - b) "*Comune*", il Comune di Trezzano sul Naviglio;
 - c) "*Decreto-Legge n. 14 del 2017*", il Decreto-Legge 20 febbraio 2017, n. 14, convertito, con modificazioni, dalla Legge 18 aprile 2017, n. 48;
 - d) "*Decreto Legislativo n. 51 del 2018*", il Decreto legislativo 18 maggio 2018, n. 51;
 - e) "*Legge n. 65 del 1986*", la Legge 7 marzo 1986, n. 65;
 - f) "*Parti*", il Comune di Trezzano sul Naviglio, la Questura di Milano, il Comando Provinciale dei Carabinieri ed il Comando Provinciale della Guardia di Finanza;
 - g) "*Prefettura*", La Prefettura Ufficio Territoriale del Governo di Milano
 - h) "*Questura*", la Questura di Milano;
 - i) "*altri uffici periferici della Polizia di Stato*", eventuali sottosezioni o commissariati;
 - j) "*Comando provinciale dei Carabinieri*", il Comando Provinciale dell'Arma dei Carabinieri di Milano;
 - k) "*altra articolazione territoriale dipendente*", Comando dell'Organizzazione territoriale dell'Arma dei Carabinieri come localmente denominato;
 - l) "*Comando Provinciale della G.d.F.*", il Comando Provinciale della Guardia di Finanza di Milano;

- m) *“altra articolazione territoriale dipendente”*, il Reparto territoriale della Guardia di Finanza come localmente denominato;
 - n) *“regolamento UE n. 679 del 2016”*, il regolamento UE 27 aprile 2016, n. 679, recante regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)”;
 - o) *“sicurezza urbana”*, il bene pubblico che afferisce alla vivibilità e al decoro delle città, da perseguire attraverso interventi di riqualificazione, anche urbanistica, sociale e culturale, e recupero delle aree o dei siti degradati, l’eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio, la promozione della cultura 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;
 - p) *“sistema di videosorveglianza”*, il sistema di videosorveglianza per la sorveglianza sistematica e automatizzata di uno specifico spazio accessibile al pubblico, effettuata con strumenti ottici o audiovisivi, per la raccolta e la conservazione di informazioni grafiche o audiovisive riguardanti tutte le persone che entrano nello spazio monitorato, identificabili in base al loro aspetto o ad altri elementi specifici, installato dal Comune di Trezzano sul Naviglio per finalità di sicurezza urbana;
 - q) *“sistema di lettura targhe”*, il sistema di videosorveglianza per il riconoscimento delle targhe di immatricolazione dei veicoli, installato dal Comune di Trezzano sul Naviglio per finalità di sicurezza stradale e per attività di Polizia Giudiziaria;
 - r) *“Codice in materia di protezione dei dati personali”*, il Codice in materia di protezione dei dati personali, di cui al Decreto legislativo 30 giugno 2003, n. 196.
2. Ai fini del presente accordo, si intende per:
- a) *“accesso”*, l’operazione di trattamento elettronico che consente di prendere visione e di estrarre copia, memorizzandola su qualunque tipo di supporto, dei dati personali raccolti dal sistema di videosorveglianza;
 - b) *“CEN”*, il Centro Elettronico Nazionale della Polizia di Stato;
 - c) *“dati resi disponibili”*, i dati personali raccolti dal Comune attraverso il sistema di videosorveglianza, resi disponibili per via telematica alle centrali operative della Questura di Milano, del Comando Provinciale dell’Arma dei Carabinieri e del Comando Provinciale della Guardia di Finanza di Milano (oppure ai Reparti territorialmente competenti di ciascuna articolazione suddetta);
 - d) *“diritti dell’interessato”*, i diritti riconosciuti alle persone interessate dal Capo III del regolamento (UE) n. 679/2016 e dal Capo II del Decreto Legislativo n. 51 del 2018;
 - e) *“SCNTT”*, il Sistema di Controllo Nazionale Targhe e Transiti, gestito dal CEN.

Art. 3

Finalità dei trattamenti

1. I dati personali raccolti dal sistema di videosorveglianza sono trattati dal Comune per il tramite del dipendente Servizio di Polizia Locale, per le finalità amministrative connesse alle funzioni ed ai compiti di sicurezza urbana attribuiti dalla Legge ai Comuni.
2. I dati personali raccolti dal sistema di lettura targhe sono trattati dal Comune per il tramite della dipendente Polizia Locale, per le finalità di sicurezza stradale, nell’ambito del territorio di competenza.
3. I dati personali raccolti con i sistemi di cui al comma 1 e comma 2, sono resi disponibili alla Polizia Locale, che può ulteriormente utilizzarli per l’assolvimento, nell’ambito territoriale di competenza, delle funzioni di Polizia Giudiziaria attribuite dall’articolo 5, comma I, lettera a) della Legge 7 marzo 1986, n. 65.
4. La Questura, il Comando Provinciale dell’Arma dei Carabinieri, e il Comando Provinciale della Guardia di Finanza, possono trattare i dati personali, resi disponibili per le finalità di cui al comma 1, per finalità di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, di cui all’articolo 1, comma 2, del Decreto Legislativo n. 51 del 2018.
5. Il CEN può trattare i dati personali di cui comma 2, comunicati dal Comune, per finalità di prevenzione, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e

la prevenzione di minacce alla sicurezza pubblica, di cui all'articolo 1, comma 2, del Decreto Legislativo n. 51 del 2018.

Art. 4

Principi generali e regole di trattamento dei dati personali

1. Le Parti concordano sulla necessità che i trattamenti per finalità amministrative dei dati personali effettuati dal Comune di Trezzano sul Naviglio attraverso il sistema di videosorveglianza ed il sistema di lettura targhe, siano compiuti nel rispetto delle regole e dei principi stabiliti dal regolamento UE n. 679/2016 e dal Codice in materia di protezione dei dati personali e che gli ulteriori trattamenti effettuati dalle Forze di Polizia siano compiuti nel rispetto delle regole e dei principi di cui al Decreto Legislativo n. 51 del 2018 e al d.P.R. 15 gennaio 2018, n. 15.
2. Il Comune di Trezzano sul Naviglio, in particolare, dà atto di aver effettuato la necessaria valutazione d'impatto sulla protezione dei dati di cui all'articolo 35 del regolamento (UE) n. 679/2016, prima di procedere al trattamento dei dati personali raccolti in modo sistematico nelle zone accessibili al pubblico, mediante il sistema di videosorveglianza per la tutela della sicurezza urbana nonché mediante il sistema di lettura targhe per il rilevamento delle violazioni in materia di circolazione stradale.
3. Il Comune di Trezzano sul Naviglio dà altresì atto di aver attuato specifiche misure che consentano di verificare l'attività espletata dal personale che accede al sistema di videosorveglianza e di lettura targhe, adottando diversificati livelli di visibilità e di trattamento delle immagini da parte del personale autorizzato, il quale è abilitato attraverso il rilascio di credenziali di autenticazione individuali.
4. Le Parti danno atto che i titolari del trattamento di cui all'articolo 5, comma 3, in conformità alle politiche interne in materia di protezione dei dati personali, effettuano la necessaria valutazione d'impatto prevista dall'articolo 23 del Decreto Legislativo n. 51 del 2018. A tal fine, i titolari del trattamento di cui all'articolo 5, comma 3, possono avvalersi della possibilità di effettuare un'unica valutazione d'impatto allorché si configurino modalità di trattamento delle immagini della videosorveglianza similari tra loro.
5. Le Parti danno altresì atto che ciascun titolare del trattamento, nell'ambito dei trattamenti di rispettiva pertinenza, assicurerà l'esercizio dei diritti degli interessati.

Art. 5

Titolari dei trattamenti

1. Il Comune di Trezzano sul Naviglio è il titolare del trattamento dei dati personali effettuato mediante il sistema di videosorveglianza per le finalità di sicurezza urbana di cui all'articolo 3, comma 1. È altresì titolare del trattamento dei dati personali effettuato mediante il sistema di lettura targhe, per le finalità di cui all'articolo 3, comma 2.
2. Il Comune di Trezzano sul Naviglio è anche titolare dell'ulteriore trattamento dei dati personali raccolti dal sistema di videosorveglianza e dal sistema di lettura targhe, resi disponibili al dipendente Servizio di Polizia Locale, per l'assolvimento, nell'ambito territoriale di competenza, degli obblighi correlati alle funzioni di polizia giudiziaria attribuite dall'articolo 5, comma 1, lettera a) della Legge 7 marzo 1986, n. 65.
3. Il Ministero dell'Interno, Dipartimento della pubblica Sicurezza, l'Arma dei Carabinieri ed il Corpo della Guardia di Finanza **sono autonomi titolari dei trattamenti dei dati personali raccolti dal sistema di videosorveglianza e messi a disposizione dal Comune**, i quali sono effettuati rispettivamente dalla Questura o altro ufficio dipendente o altra articolazione periferica della Polizia di Stato, dal Comando Provinciale dell'Arma dei Carabinieri o altra articolazione territoriale dipendente e dal Comando Provinciale della Guardia di Finanza o altro Reparto territoriale dipendente, per le finalità di cui all'articolo 3, comma 4.
4. Il Ministero dell'interno, dipartimento della pubblica sicurezza, è autonomo titolare del trattamento dei dati personali raccolti dal sistema di lettura targhe e comunicati dal Comune, effettuato dal CEN mediante l'SCNTT, per le finalità di cui all'articolo 3, comma 5.
5. Le Parti danno atto che i Titolari dei trattamenti, ciascuno per l'ambito di rispettiva competenza, adottano, in conformità a quanto previsto dall'Allegato A, accluso alla presente convenzione, misure tecniche e organizzative idonee per garantire un livello di sicurezza adeguato al rischio di violazioni di

sicurezza che comportino, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzati ai dati personali comunque trattati.

Art. 6

Autorizzati ai trattamenti

1. Le persone che agiscono sotto l'autorità diretta dei titolari del trattamento non possono avere accesso ai dati personali se sono state previamente autorizzate e istruite in tal senso. L'autorizzazione è documentata per iscritto e descrive nel dettaglio l'ambito di trattamento consentito, definendo diversi livelli di visibilità e trattamento dei dati in funzione dei compiti attribuiti ai singoli operatori.
2. L'autorizzazione al trattamento di cui al comma 1 è adottata:
 - per il Comune, nell'ambito del personale del Corpo (o Servizio) di Polizia Locale, dal Comandante (o dal Responsabile del Servizio);
 - per il Ministero dell'interno - Dipartimento della sicurezza pubblica, dal Questore (o dal Dirigente di altro ufficio periferico della Polizia di Stato) o, su sua delega, da altra persona da questi nominata nell'ambito del personale della Polizia di Stato dipendente;
 - per l'Arma dei Carabinieri, dal Comandante Provinciale o, su sua delega, dal Comandante del Reparto Operativo, ovvero dal Comandante del Reparto Territoriale da cui dipende la centrale operativa, nell'ambito del personale dipendente;
 - per la Guardia di Finanza dal Comandante Provinciale o, su sua delega, dal Comandante del Reparto territoriale dipendente.

Capo II

Caratteristiche generali del sistema di videosorveglianza e del sistema di lettura targhe

Art. 7

Caratteristiche tecniche del sistema di videosorveglianza

1. Le caratteristiche tecniche del sistema di videosorveglianza e del sistema di lettura targhe sono definite dal documento in Allegato B al presente accordo, ove può essere indicata anche l'ubicazione delle telecamere. Le Parti danno atto che le informazioni relative all'ubicazione delle telecamere potranno essere fornite anche attraverso modalità di georeferenziazione su cartografia digitale, integrate nel sistema.
2. Le Parti danno atto che il sistema di videosorveglianza è configurato in modo da consentire alle sale o centrali operative della Questura (o altro ufficio periferico della Polizia di Stato), del Comando Provinciale dell'Arma dei Carabinieri (o altra articolazione territoriale dipendente) e del Comando Provinciale del Corpo della Guardia di finanza (o altra articolazione territoriale dipendente) di accedere in tempo reale (*live*) al predetto sistema e alle immagini da esso riprese secondo le modalità selettive, individuate dall'articolo 9, commi 2 e 3.
3. Le Parti danno inoltre atto che gli accessi e le operazioni sul server ove sono conservate le registrazioni del sistema di videosorveglianza, effettuati dal personale autorizzato dal Comune con le modalità di cui all'articolo 6, comma 2, sono registrati in appositi file di log, non modificabili, conservati dal Comune **per 3 anni** dall'accesso e dall'operazione, resi accessibili per la verifica della liceità del trattamento, del controllo interno e nell'ambito del procedimento penale.

Art. 8

Informativa concernente il sistema di videosorveglianza

1. Il Comune assicura che l'informativa agli interessati che stanno per accedere in una zona videosorvegliata o nel raggio d'azione del lettore targhe è fornita, ai sensi dell'articolo 13 del Regolamento (UE) n. 679/2016, attraverso la collocazione di cartelli di avvertimento conformi al modello semplificato di informativa "minima" definita dal Garante per la protezione dei dati personali (primo livello). Tale informativa "minima" rimanda all'informativa completa e dettagliata di cui al menzionato articolo 13 (secondo livello), messa a conoscenza degli interessati mediante affissione

nell'albo pretorio, nonché pubblicazione sul sito web istituzionale del Comune accessibile anche con QR-code inserito nel cartello di avvertimento.

2. L'attivazione del collegamento con le centrali/sale operative della Polizia di Stato, dell'Arma dei Carabinieri e del Corpo della Guardia di Finanza è resa nota agli interessati mediante l'informativa (di primo e secondo livello) di cui al comma 1.

Art. 9

Collegamento del sistema di videosorveglianza alle sale o centrali operative della Questura, del Comando Provinciale dell'Arma dei Carabinieri e del Corpo della Guardia di Finanza

1. Le Parti danno atto del fatto che il collegamento del sistema di videosorveglianza alle soluzioni tecnologiche adottate dalle sale o centrali operative della Questura (o altro ufficio periferico della Polizia di Stato), del Comando Provinciale dell'Arma dei Carabinieri (o altra articolazione territoriale dipendente) e del Comando Provinciale del Corpo della Guardia di Finanza (o altra articolazione territoriale dipendente), avviene per mezzo di una rete telematica dedicata proprietaria del Comune di Trezzano sul Naviglio.
2. Il collegamento consente al personale delle predette sale o centrali operative, per le esigenze di prevenzione e repressione dei reati e di tutela dell'ordine e della sicurezza pubblica, di accedere alle telecamere e visionare le immagini in tempo reale (*live*). Il collegamento consente al personale autorizzato delle sale o centrali operative del Comando Provinciale del Corpo della Guardia di Finanza (o altra articolazione territoriale dipendente) di accedere, per finalità di prevenzione e repressione della contraffazione e falsificazione di prodotti, nonché per la prevenzione di altri fenomeni illeciti suscettibili di determinare turbative del libero utilizzo degli spazi pubblici, di accedere alle telecamere e visionare le immagini in tempo reale (*live*), in presenza degli eventi o delle situazioni indicate nell'Allegato D, accluso alla presente Convenzione.
3. Il collegamento consente al personale autorizzato delle sale o centrali operative di cui al comma 1 nonché eventualmente ad altro personale appositamente individuato dipendente dalla Questura o dal Comando Provinciale dell'Arma dei Carabinieri ovvero o del Corpo della Guardia di Finanza, di accedere alle immagini in differita ed estrarne copia, con connessione da remoto al server, ove sono conservate le registrazioni raccolte dal sistema di videosorveglianza comunale.
4. Le Parti danno inoltre atto che la Questura (o altro ufficio periferico della Polizia di Stato), il Comando Provinciale dell'Arma dei Carabinieri (o altra articolazione territoriale dipendente) ed il Comando Provinciale del Corpo della Guardia di Finanza (o altro Reparto territoriale dipendente) adottano diversificati livelli di visibilità e di trattamento delle immagini da parte del personale autorizzato di cui all'articolo 6, il quale è abilitato, attraverso il rilascio di credenziali di autenticazione individuali, a compiere le sole operazioni correlate ai compiti assegnati. Le credenziali per accedere al server di cui al comma 2 sono rilasciate in forma anonima dal Comune e sono gestite direttamente dagli "amministratori" di ciascuna Forza di Polizia.
5. Le operazioni di visione delle immagini di cui ai commi 2 e 3 e le esigenze che le hanno rese necessarie sono annotate, anche in modalità automatizzata, nel registro della sala o centrale operativa e delle altre unità operative interessate.
6. Le Parti danno altresì atto che gli accessi e le operazioni effettuate dal personale della Questura (o altro ufficio periferico della Polizia di Stato), del Comando Provinciale dell'Arma dei Carabinieri (o altra articolazione territoriale dipendente) e del Comando Provinciale del Corpo della Guardia di Finanza (o altro Reparto territoriale dipendente) sul server comunale sono registrati in appositi file di log, non modificabili, conservati dal Comune per 3 anni dall'accesso e dall'operazione, resi accessibili per la verifica della liceità del trattamento, del controllo interno e nell'ambito del procedimento penale.

Art. 10

Personale addetto alla gestione e manutenzione del sistema di videosorveglianza

1. Le Parti danno atto che la gestione, la manutenzione e l'aggiornamento del sistema di videosorveglianza e del sistema di lettura targhe sono garantite dal Comune, quale proprietario del

sistema, attraverso personale tecnico appositamente incaricato, al quale non è consentito accedere alle risorse informative memorizzate nel sistema.

2. AI termini di ciascun intervento di manutenzione, il responsabile dell'operazione di manutenzione rilascia al Comune una dichiarazione scritta relativa all'attività svolta.
3. Le Parti danno atto che con riferimento alla comunicazione del Comune dei dati raccolti dal sistema di lettura targhe, gli interventi che rendano necessario l'accesso fisico al server collettore ubicato in Questura (o in altro ufficio periferico della Polizia di Stato), siano previamente concordati ed eseguiti alla presenza dell'amministratore di sistema (o altro tecnico) della Questura. In tali casi il personale tecnico incaricato dal Comune rilascia attestazione scritta delle operazioni eseguite.
4. Le Parti danno atto che il Comune assicurerà l'adeguamento del sistema di lettura targhe alle prescrizioni tecniche impartite dal Dipartimento della pubblica sicurezza, per garantire il collegamento telematico in caso di interventi di aggiornamento tecnologico riguardanti l'SCNTT.

Capo III

Trattamento dei dati personali per finalità di sicurezza urbana

Art. 11

Ubicazione del server utilizzato per i trattamenti effettuati per finalità di sicurezza urbana

1. Le Parti danno atto che il server presso il quale sono memorizzati i dati personali raccolti dal sistema di videosorveglianza per finalità di sicurezza urbana, resi disponibili alla Questura (o altro ufficio periferico della Polizia di Stato), al Comando provinciale (o altra articolazione territoriale dipendente) e al Comando Provinciale della Guardia di Finanza (o altro Reparto territoriale dipendente), è ubicato presso la sala CED dell'Ufficio Sistemi Informativi del Comune di Trezzano sul Naviglio, accessibile soltanto al personale autorizzato dal responsabile del suddetto Servizio.

Art. 12

Rilevazione delle targhe dei veicoli e modalità di comunicazione al SCNTT

1. Le Parti convengono che il sistema di lettura targhe comunale può essere interconnesso all'SCNTT attraverso un collegamento telematico dedicato con un server collettore installato presso la Questura (o altro ufficio periferico della Polizia di Stato) con le modalità tecniche di interfacciamento definite dal CEN.

Art. 13

Termine di conservazione dei dati raccolti per finalità di sicurezza urbana

1. La conservazione dei dati, delle informazioni e delle immagini, raccolti per le finalità di sicurezza urbana, attraverso il sistema di videosorveglianza è limitata, ai sensi dell'articolo 6, comma 8, del Decreto Legge 23 febbraio 2009, n. 11, convertito, con modificazioni, dalla Legge 23 aprile 2009, n. 38, ai **sette giorni** successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione, quali quelle connesse allo svolgimento di eventuali attività di indagine delegate dall'Autorità Giudiziaria. Decorso i termini predetti, le immagini sono cancellate automaticamente.

Capo IV

Disposizioni finali

Art. 14

Risoluzione delle controversie

1. Le Parti si impegnano a risolvere bonariamente tutte le controversie che dovessero eventualmente insorgere dall'applicazione del presente protocollo. Le eventuali controversie tra le Parti derivanti dalla interpretazione, gestione o esecuzione della presente convenzione sono deferite, in via esclusiva, al Foro di Milano.

Art. 15

Clausola invarianza finanziaria

1. Dalla firma del presente accordo attuativo, non derivano nuovi e maggiori oneri per l'Erario e all'attuazione delle relative disposizioni si provvede con le risorse umane, finanziarie e strumentali disponibili a legislazione vigente.

Art. 16

Durata e modifica della presente Convenzione

1. La presente Convenzione ha una durata di **2 anni** dalla data della sua sottoscrizione e si considera rinnovata tacitamente, qualora una delle Parti non notifichi, almeno 90 giorni prima dalla sua scadenza, la volontà di recedere.
2. Le Parti concordano di modificare le clausole della presente Convenzione, ove ciò si renda necessario per effetto di norme o direttive di settore sopravvenute.
3. La presente Convenzione si intende vigente ed efficace anche per future implementazioni o spostamenti delle telecamere rispetto all'ubicazione prevista nel documento in Allegato B.

Art. 17

Sottoscrizione

1. Il presente protocollo è sottoscritto con firma digitale ed è soggetto agli obblighi di pubblicazione ai sensi dell'articolo 23, comma 1, lettera d), del Decreto Legislativo 14 marzo 2013, n. 33

Il Sindaco di Trezzano sul Naviglio

(Documento firmato digitalmente ai sensi e con gli effetti degli artt. 20 e 21 del D. Lgs. 82/2005)

Il Questore di Milano

(Documento firmato digitalmente ai sensi e con gli effetti degli artt. 20 e 21 del D. Lgs. 82/2005)

Il Comandante dei Carabinieri

(Documento firmato digitalmente ai sensi e con gli effetti degli artt. 20 e 21 del D. Lgs. 82/2005)

Il Comandante della Guardia di Finanza

(Documento firmato digitalmente ai sensi e con gli effetti degli artt. 20 e 21 del D. Lgs. 82/2005)

Allegato A

ELENCO DELLE MISURE TECNICHE CONCERNENTI LA SICUREZZA DEI SISTEMI DI VIDEOSORVEGLIANZA E DI LETTURA TARGHE

Il titolare del trattamento, in relazione alle tecnologie da esso impiegate per il trattamento dei dati personali raccolti dal sistema di videosorveglianza e dal sistema di lettura targhe, previa valutazione di rischi, adotta le misure volte a:

- a) proteggere fisicamente i dati adottando idonee misure per il controllo degli accessi (es. serrature di sicurezza, badge elettronico, sistemi di riconoscimento biometrico, ecc.) e per assicurare l'affidabilità dell'infrastruttura (es. gruppi di continuità, sistemi UPS, impianti antintrusione, antincendio, antiallagamento, ecc.);
- b) proteggere i flussi di comunicazione del sistema di videosorveglianza e di lettura targhe attraverso la presenza di firewall perimetrali, anche con funzioni di antimalware, antivirus, antispyware, al fine di evitare possibili accessi non autorizzati;
- c) negare alle persone non autorizzate l'accesso ai dispositivi utilizzati per il trattamento dei dati;
- d) impedire che i supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate;
- e) impedire che i dati raccolti dal sistema di videosorveglianza e dal sistema di lettura targhe, siano trattati senza autorizzazione e che sia presa visione senza autorizzazione dei dati personali conservati, o che gli stessi siano modificati o cancellati o trasmessi senza autorizzazione;
- f) garantire, in conformità a quanto stabilito dall'art. 9, commi 6 e 7, della presente Convenzione e dalle specifiche misure di sicurezza previste dall'SCNTT, che le persone autorizzate abbiano accesso ai dati raccolti dal sistema di videosorveglianza e dal sistema di lettura targhe, secondo livelli di visibilità differenziati in funzione della necessità di accedere ai dati personali strettamente necessari in base al ruolo posseduto, mediante il rilascio di credenziali di autenticazione individuali (anche adottando adeguate procedure di password policy);
- g) garantire che sia possibile verificare e stabilire quali dati sono stati trattati dal sistema di videosorveglianza e dal sistema di lettura targhe, e quando, da chi e per quale scopo essi sono stati trattati (procedure di raccolta e analisi dei log);
- h) impedire, anche mediante meccanismi di crittografia, che i dati durante il trasferimento su rete telematica, siano letti, copiati, modificati o cancellati senza autorizzazione;
- i) garantire che, in caso di interruzione, i sistemi di videosorveglianza e di lettura targhe possano essere riattivati attraverso idonee procedure di backup (copie di sicurezza opportunamente crittografate e conservate in modo sicuro), allo scopo di assicurarne la disponibilità, l'integrità e il recupero a seguito di un evento avverso (danneggiamento ovvero a causa di un malfunzionamento);
- j) garantire l'affidabilità, accertandosi che eventuali anomalie nel funzionamento del sistema di videosorveglianza e di lettura targhe, siano adeguatamente segnalate;
- k) monitorare l'efficacia delle sopra citate misure di sicurezza garantendone l'osservanza.

Allegato C

ELENCO DEGLI EVENTI E DELLE SITUAZIONI RILEVANTI PER L'ACCESSO DA PARTE DELLE SALE O CENTRALI OPERATIVE DELLA POLIZIA DI STATO E DELL'ARMA DEI CARABINIERI

- A. Il personale delle sale o delle centrali operative della Questura (o altro ufficio periferico della Polizia di Stato) o del Comando Provinciale dell'Arma dei Carabinieri (o altra articolazione territoriale dipendente) è autorizzato ad accedere alle telecamere e visionare le immagini in tempo reale (*live*), in presenza degli eventi o delle situazioni qui di seguito riportate:
1. manifestazioni pubbliche, anche se non preavvisate;
 2. manifestazioni sportive;
 3. eventi che si svolgono in luogo pubblico che richiamano un significativo afflusso di persone;
 4. esecuzione di servizi di ordine e sicurezza pubblica disposti dal Questore con ordinanza di cui all'articolo 37 del Decreto del Presidente della Repubblica 28 ottobre 1985, n. 782;
 5. esecuzione di servizi coordinati di controllo del territorio, disposti dal Questore o dal Comandante Provinciale dell'Arma dei Carabinieri;
 6. servizi di controllo delle infrastrutture del trasporto pubblico urbano, ferroviario, dei porti e degli aeroporti e delle aree ad esse limitrofe;
 7. situazioni oggetto di richieste di intervento urgente pervenute al Numero unico di emergenza europeo 112 (NUE 112), ovvero ad altri numeri di emergenza nelle Regioni in cui il NUE 112 non è stato ancora attivato;
 8. svolgimento di operazioni di polizia giudiziaria;
- B. Il personale delle sale o delle centrali operative della Questura (o altro ufficio periferico della Polizia di Stato) o del Comando Provinciale dell'Arma dei Carabinieri (o altra articolazione territoriale dipendente) è autorizzato ad accedere e visionare le immagini in tempo reale (*live*), riprese da telecamere del sistema di videosorveglianza comunale, situate in aree urbane, preventivamente individuate con apposita direttiva del Prefetto, adottata sulla base del parere reso dal Comitato provinciale per l'ordine e la sicurezza pubblica in ragione di esigenze di prevenzione e repressione dei fenomeni di criminalità. Con la predetta direttiva, il Prefetto di XXXXXX, sulla base del parere reso dal Comitato provinciale per l'ordine e la sicurezza pubblica, determina anche il periodo di tempo durante il quale può essere eseguito l'accesso o la visione alle immagini. Il predetto periodo può essere prorogato per motivate esigenze di tutela dell'ordine e della sicurezza pubblica.

Allegato D
ELENCO DEGLI EVENTI E DELLE SITUAZIONI
RILEVANTI PER L'ACCESSO DA PARTE DELLE SALE O CENTRALI OPERATIVE
DELLA GUARDIA DI FINANZA

- A. Il personale delle sale o centrali operative del Comando Provinciale del Corpo della Guardia di Finanza (o altra articolazione territoriale dipendente) è autorizzato ad accedere alle telecamere e visionare le immagini in tempo reale (*live*), in presenza degli eventi o delle situazioni qui di seguito riportate:
1. manifestazioni sportive;
 2. pubblici spettacoli e trattenimenti;
 3. eventi a carattere internazionale e eventi a carattere nazionale che richiamano un significativo afflusso di persone;
 4. svolgimento di fiere e mercati su aree pubbliche;
 5. specifici servizi di controllo delle infrastrutture del trasporto pubblico urbano, ferroviario, dei porti e degli aeroporti e delle aree ad esse limitrofe;
 6. esecuzione di servizi di ordine e sicurezza pubblica disposti dal Questore con ordinanza di cui all'articolo 37 del Decreto del Presidente della Repubblica 28 ottobre 1985, n. 782;
 7. specifici servizi di controllo delle aree in cui sono concentrati snodi organizzativi e di smistamento delle reti di distribuzione della merce illegale (contraffatta e/o pericolosa), nell'ambito di opifici, fabbriche ovvero aree industriali, artigianali e commerciali;
 8. specifici servizi di controllo eseguiti lungo aree urbane ed extraurbane di particolare interesse per i flussi commerciali, anche per la prossimità a zone industriali e poli produttivi;
 9. situazioni oggetto di richieste di intervento urgente pervenute al numero di pubblica utilità "117";
 10. svolgimento di operazioni di polizia giudiziaria.
- B. Il personale delle sale operative del Comando Provinciale della Guardia di Finanza (o altra articolazione territoriale dipendente) è autorizzato ad accedere e visionare le immagini in tempo reale (*live*), riprese da telecamere del sistema di videosorveglianza comunale, situate in aree urbane, preventivamente individuate con apposita direttiva del Prefetto, adottata sulla base del parere reso dal Comitato provinciale per l'ordine e la sicurezza pubblica in ragione di esigenze di prevenzione e repressione della contraffazione e falsificazione dei prodotti, nonché per la prevenzione di altri fenomeni illeciti suscettibili di determinare turbative del libero utilizzo degli spazi pubblici.
- C. Con la predetta direttiva, il Prefetto di Milano, sulla base del parere reso dal Comitato provinciale per l'ordine e la sicurezza pubblica, determina anche il periodo di tempo durante il quale può essere eseguito l'accesso o la visione alle immagini. Il predetto periodo può essere prorogato per motivate esigenze di tutela dell'ordine e della sicurezza pubblica.

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

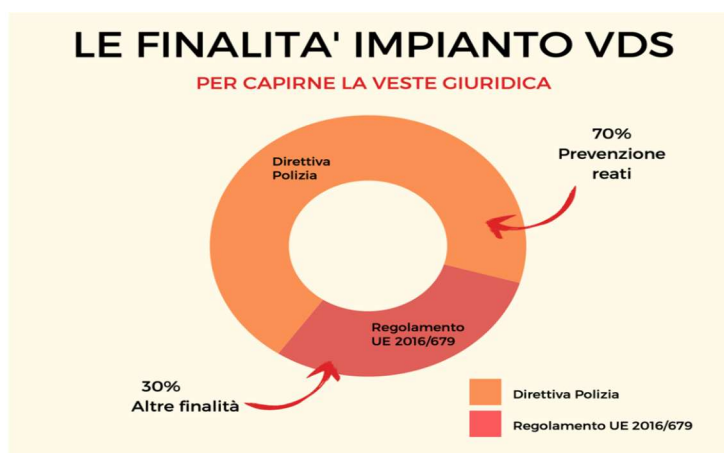
Con le linee generali del 24 gennaio 2018 il pacchetto sicurezza Minniti (dl 14/2017) ha subito una brusca accelerazione. Era, infatti, necessario definire la cornice organica degli strumenti attraverso i quali i diversi livelli di governo ma anche i soggetti privati sono chiamati a cooperare per realizzare 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 (licenze 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 Brescia
Provincia di Brescia

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: _____

Redatto da: _____

Validato da: _____

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>

GRUPPO
 EVENTUALE

Ai sensi
del dl
116/20
25

FASE
D

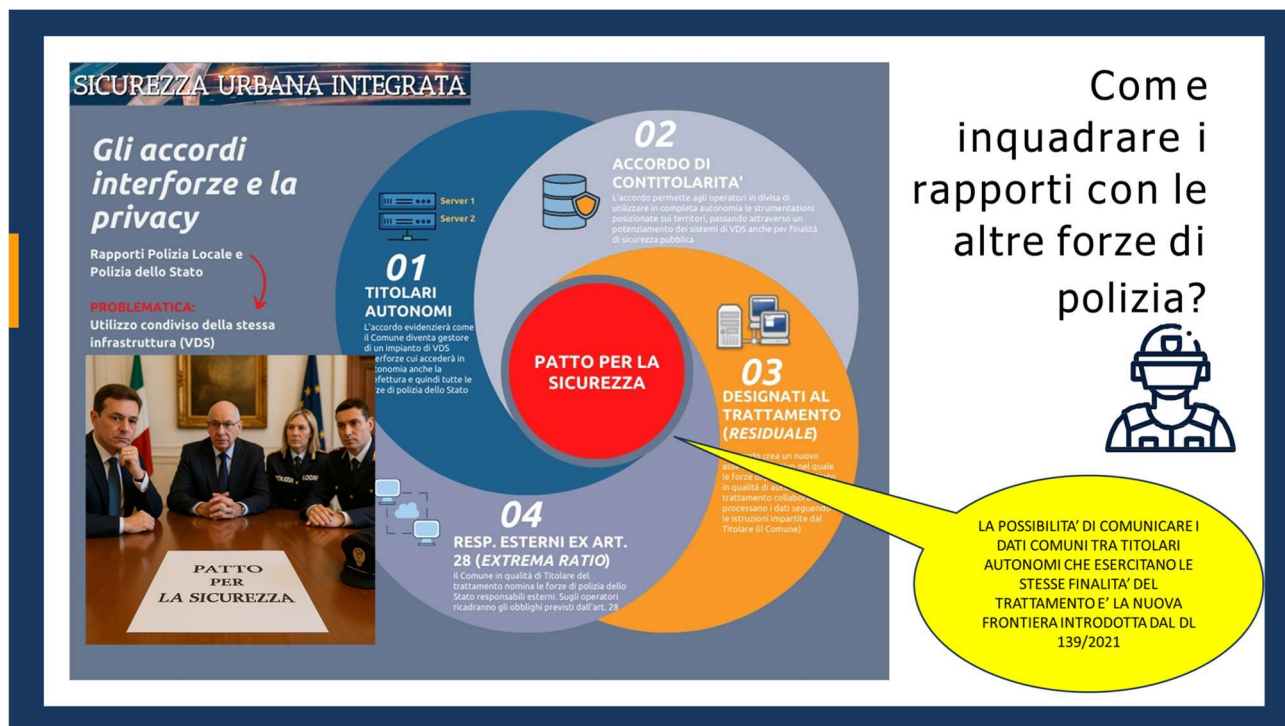
LA TRASPARENZA E LA RENDICONTAZIONE PERIODICA



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 Selea. 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

I PASSI SUCCESSIVI ALLA STESURA DI UN PROGETTO DI SICUREZZA URBANA INTEGRATA

Guida per gli operatori

IL PROGETTO DI SICUREZZA URBANA INTEGRATA

CHE COS'È?



Un progetto di sicurezza urbana integrata è un documento che racchiude il percorso di allineamento dell'ente alle varie normative di settore (GDPR, Direttiva Polizia, Pacchetto Sicurezza, Legge 205/2021, Regolamento UE 2024/1689 - AI Act, Legge n. 132/2025 etc.) per una corretta gestione degli impianti di videosorveglianza in ottica di sicurezza urbana integrata.

Oltre a costituire un importante manifesto di intenti per l'amministrazione incrementa l'accountability GDPR (il *punteggio privacy* dell'amministrazione) poiché partendo da una descrizione dello stato di partenza degli impianti di videosorveglianza dell'ente, dei suoi sistemi informatici, dei rapporti in essere con le interforze, nonché degli obiettivi politici, *facilita* l'allineamento normativo mettendo a bordo un progetto di architettura privacy che da maggiore robustezza agli obiettivi dell'amministrazione e costituisce il punto di partenza per la messa a norma dei sistemi.

COM'È STRUTTURATO?

Il progetto è un documento che l'amministrazione riceverà sia in formato editabile (.doc) sia in versione stampata.

Si compone di un certo numero di allegati, alcuni variabili e rilasciati in base al contesto di riferimento e alle necessità dell'amministrazione, altri fissi sempre presenti, ovvero:

1. Una matrice di Patto per la Sicurezza per la condivisione degli obiettivi con la Prefettura;
2. Una matrice di accordo fra le forze di polizia;
3. Una modello di regolamento di videosorveglianza;
4. Uno esempio di registro dei trattamenti relativo alla vds da innestare nel registro complessivo dell'ente.

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 tempore 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.
- 4-bis. FRIA (Valutazione d'impatto sui diritti fondamentali): se i sistemi di videosorveglianza utilizzano funzionalità AI (video-analisi, lettura targhe automatica, tracciamento movimenti, riconoscimento anomalie), l'ente è tenuto alla redazione della FRIA ai sensi dell'art. 27 AI Act. La Polizia Locale è spesso utilizzatore inconsapevole di tecnologie che hanno a bordo sistemi di intelligenza artificiale, quindi è fondamentale mappare tutti i sistemi. La FRIA va redatta prima della messa in esercizio dei sistemi che usano intelligenza artificiale e aggiornata periodicamente.

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

Regolamento per la disciplina del sistema di videosorveglianza

INDICE

Art. 1 – Oggetto e base giuridica

Art. 2 – Principi generali

Art. 3 – Soggetti

Art. 4 – Informativa

Art. 5 – Finalità dei sistemi e architettura degli impianti presenti

Art. 6 – Trattamento e conservazione dei dati

Art. 7 – Modalità di raccolta dei dati

Art. 8 – Diritti dell'interessato

Art. 9 – Accesso ai filmati

Art. 10 – Sicurezza dei dati

Art. 11 – Cessazione del trattamento dei dati

Art. 12 – Tutela amministrativa e giurisdizionale

Art. 13 – Disciplinare-programma

Art. 14 – Norme finali

Art. 1 – Oggetto e base giuridica

1. Il presente regolamento disciplina le modalità di raccolta, elaborazione, conservazione ed accesso dei dati personali mediante sistemi di videosorveglianza gestiti, nell'ambito del proprio territorio, dal Comune di _____ ed ha lo scopo di stabilire norme tecniche e organizzative di dettaglio e di concorrere a definire la base giuridica, le finalità e i mezzi del trattamento.
2. Il presente regolamento, quale atto amministrativo generale, come definito dall'articolo 12 del Decreto legislativo 14 marzo 2013, n. 33, valorizza la base giuridica del trattamento stesso a norma dell'articolo 2-ter, comma 1, del Decreto legislativo 30 giugno 2003, n. 196 garantendo la liceità del trattamento prevista dall'articolo 6 del Regolamento UE 2016/679.
3. Costituisce videosorveglianza quel complesso di strumenti finalizzati alla vigilanza in remoto, ossia a distanza, mediante dispositivi di ripresa video, collegati ad un centro di controllo.
4. Le immagini, qualora rendano le persone identificate o identificabili, costituiscono dati personali. In tali casi la videosorveglianza incide sul diritto delle persone alla propria riservatezza.
5. Con il presente regolamento si garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di sistemi di videosorveglianza gestiti e impiegati dal Comune nel proprio territorio, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.
6. Ai fini delle definizioni si deve fare riferimento al Regolamento Ue 2016/679 (*“Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)”*), d'ora in poi GDPR - General Data Protection Regulation), al novellato D.lgs. 196/2003 (recante il *“Codice in materia di protezione dei dati personali”*, così come modificato dal D.lgs. 101/2018) e al D.lgs. 51/2018 (recante l'*“Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio”*), d'ora in poi *“Direttiva polizia”*).
7. Il presente regolamento, ai sensi degli articoli 5 e 6 del GDPR e dell'articolo 3 della Direttiva Polizia, stabilisce norme di dettaglio rilevanti finalizzate ad attuare, riguardo i trattamenti dei dati personali effettuati mediante l'uso di sistemi di videosorveglianza, i principi, come definiti nei richiamati articoli 5 e 3, di liceità, correttezza, trasparenza, limitazione delle finalità e minimizzazione dei dati, esattezza, limitazione della conservazione, integrità riservatezza e responsabilizzazione.
8. Il Comune di _____ promuove la sottoscrizione di protocolli di intesa, patti per la sicurezza e patti per l'attuazione, convenzioni o accordi comunque denominati con soggetti pubblici e soggetti privati. È in ogni caso garantita la comunicazione a norma dell'articolo 2-ter, comma 2, del D.lgs. 196/2003, di dati all'Autorità Giudiziaria e alle Forze di polizia, per il perseguimento delle medesime finalità di cui al successivo articolo 5 del presente regolamento.

Art. 2 - Principi generali

1. Ai sensi della vigente normativa, i Comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per tutela della sicurezza urbana, la cui definizione è stata da ultimo riformulata dal D.L. 14/2017, convertito nella legge 18 aprile 2017 n. 48, all'art. 4 e definita come *“il bene pubblico che afferisce alla vivibilità e al decoro delle città da perseguire anche attraverso interventi di riqualificazione anche urbanistica, sociale e culturale, e recupero delle aree o dei siti degradati, l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio la promozione della cultura 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”* da potenziare con accordi/patti locali ispirati ad una logica di gestione consensuale ed integrata della sicurezza. Si riassumono di seguito i principi per il trattamento dei dati che saranno garantiti scrupolosamente:
 - Principio di liceità: il trattamento di dati personali effettuato attraverso sistemi di videosorveglianza da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali. Esso, infatti, è necessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui il Comune e il Comando di Polizia Municipale sono investiti.
 - Principio di necessità: i sistemi di videosorveglianza sono configurati per l'utilizzazione al minimo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
 - Principio di proporzionalità: nel commisurare la necessità del sistema di videosorveglianza al grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra una effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano valutate insufficienti o inattuabili rispetto alle finalità perseguite.
 - Principio di finalità: gli scopi perseguiti devono essere determinati, espliciti e legittimi. È consentita la videosorveglianza come misura complementare volta a tutelare la sicurezza urbana anche nell'ambito di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, o comunque con lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti.

Art. 3 – Soggetti

1. Titolare per il trattamento dei dati è il Comune di _____.
2. Designato al trattamento dei dati rilevati con apparecchi di videosorveglianza è il Comandante della polizia locale per le telecamere connesse alla centrale operativa. Gli altri

dirigenti/responsabili per le telecamere dedicate alla tutela del patrimonio nella loro disponibilità.

3. I designati individuano e nominano, con proprio provvedimento, gli autorizzati alla gestione dell'impianto nel numero ritenuto sufficiente a garantire il corretto funzionamento del servizio.
4. Con l'atto di nomina ai singoli autorizzati sono affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi.
5. Sono designati dal Titolare del trattamento l'amministratore o gli amministratori di sistema, oltre che i responsabili del trattamento dei dati ai sensi dell'art. 28 del GDPR.
6. In relazione alle finalità di attuazione di un sistema di sicurezza integrata, di cui al successivo articolo 5 del presente regolamento, poiché finalità e mezzi saranno determinati congiuntamente dai soggetti coinvolti, il Comune potrà essere contitolare del trattamento, ai sensi dell'articolo 26 del GDPR nonché articolo 17 della direttiva polizia.

Art. 4 – Informativa

1. I soggetti interessati che stanno per accedere o che si trovano in una zona videosorvegliata sono informati mediante cartelli, nei casi specificamente previsti dalla normativa vigente.
2. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, sono installati più cartelli.
3. Sul sito istituzionale del Comune, a cura del Comando di Polizia Municipale, in un'apposita area dedicata oltre che presso gli uffici individuati, è disponibile inoltre l'informativa (sinteticamente richiamata dai cartelli installati sul territorio) concernente le finalità degli impianti di videosorveglianza, la modalità di raccolta e conservazione dei dati e le modalità di diritto di accesso dell'interessato secondo quanto previsto dal GDPR e dalla direttiva polizia.

Art. 5 – Finalità dei sistemi e architettura degli impianti presenti

1. Le finalità perseguite mediante l'attivazione di sistemi di videosorveglianza sono conformi alle funzioni istituzionali attribuite ai Comuni secondo quanto richiamato dalla normativa vigente in materia. L'eventuale utilizzo del sistema di videosorveglianza per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, con sistematico accesso da parte delle forze di polizia a competenza generale, dovrà essere specificamente disciplinato con appositi atti, patti e convenzioni.
2. Il presente regolamento valorizza la base giuridica del trattamento a norma dell'articolo 2-*ter* del d.lgs. 196/2003. Il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato per finalità di:
 - attuazione di un sistema di sicurezza integrata ai sensi dell'art. 2 del D.L. 14/2017; tutela della sicurezza urbana e della sicurezza pubblica; tutela degli operatori e del patrimonio comunale; tutela della protezione civile e della sanità pubblica; tutela della sicurezza stradale; tutela ambientale e polizia amministrativa; prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali; arresto in flagranza differito (art. 10 co. 6-*quater* del D.L. 14/2017).
3. Il sistema di videosorveglianza implica il trattamento di dati personali che possono essere rilevati da telecamere tradizionali eventualmente munite di algoritmi di analisi video,

metadattazione, conteggio delle persone e verifica dei comportamenti o varchi lettura targhe connessi a black-list o altre banche dati, in grado di verificare la regolarità di un transito di un veicolo.

4. Il Comune promuove, per quanto di propria competenza, con deliberazione della Giunta Comunale di cui al successivo art. 13, il coinvolgimento dei privati per la realizzazione di singoli impianti di videosorveglianza, orientati comunque su aree o strade pubbliche o ad uso pubblico, nel rispetto dei principi di cui al presente regolamento, previa valutazione di idoneità dei siti e dei dispositivi, normalmente senza connessioni al sistema centrale e senza possibilità di accesso ai filmati, ma con connessioni preferibilmente stand alone (nel significato di “sistema autonomo chiuso”). I privati interessati assumono su di sé ogni onere per acquistare le attrezzature e renderle operative in conformità alle caratteristiche tecniche dell'impianto pubblico, le mettono a disposizione dell'ente a titolo gratuito, senza mantenere alcun titolo di ingerenza sulle immagini e sulla tecnologia connessa. Il Comune può assumere su di sé gli oneri per la manutenzione periodica e la responsabilità della gestione dei dati raccolti.
5. Nei casi di cui al comma precedente, in accordo con il Comune e previa stipula di apposita convenzione, i soggetti privati che hanno ceduto in comodato i propri impianti di videosorveglianza all'ente possono decidere, con oneri a proprio carico, di affidare il controllo in tempo reale delle immagini ad un istituto di vigilanza privato, con il compito di allertare ed interessare in tempo reale le forze di polizia in caso di situazioni anomale.
6. Il Comune può dotarsi di body-cam (telecamere a corpo), dash-cam (telecamera su auto), droni volanti, telecamere riposizionabili (anche del tipo fototrappola), altri dispositivi mobili (anche con generazione di allarmi da remoto per il monitoraggio attivo). Le modalità di impiego dei dispositivi in questione sono stabilite nel disciplinare-programma di cui all'art. 13 del presente regolamento e/o con apposito provvedimento del Comando di Polizia Municipale.
7. Fermo restando la competenza tecnica del Cosp (Comitato provinciale per l'ordine e la sicurezza pubblica) e della Prefettura-Ufficio Territoriale del Governo (Utg), ogni implementazione o modifica del sistema di videosorveglianza mediante l'introduzione di nuove tecnologie dovrà essere preventivamente asseverato con una determinazione tecnica/amministrativa di Giunta, in grado di evidenziare e attuare i fondamentali principi del GDPR e della direttiva polizia ovvero la rispondenza del proposto intervento ai principi di legalità, proporzionalità, necessità, finalità e minimizzazione del trattamento. In tale caso si provvederà, in conformità a quanto prescritto nel periodo precedente, a verificare che le novità siano ricomprese nella DPIA (Valutazione d'impatto della protezione dei dati) e, in caso negativo, si procederà al suo aggiornamento.

Art. 6 – Trattamento e conservazione dei dati

1. I dati personali oggetto di trattamento effettuato con strumenti elettronici nel rispetto delle misure minime indicate dalla normativa relativa alla protezione delle persone fisiche sono:
 - a) trattati in modo lecito e secondo correttezza;
 - b) raccolti e registrati per le finalità di cui al precedente art. 5 (“*Finalità dei sistemi e architettura degli impianti presenti sul territorio comunale*”) e resi utilizzabili per operazioni compatibili con tali scopi;
 - c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;

- d) conservati per le telecamere collegate alla centrale operativa per un periodo ordinariamente non superiore a 7 giorni successivi alla rilevazione. Tale termine potrà essere esteso per finalità di indagine, mediante un ulteriore atto in applicazione del D.L. 8 ottobre 2021, n. 139 (conv. Legge 205/2021). Di tale ulteriore conservazione se ne darà notizia nell'informativa completa ai sensi dell'art. 13 del GDPR pubblicata sul sito internet comunale oltre che nel disciplinare-programma;
 - e) conservati per le telecamere a tutela del solo patrimonio comunale (o per altre telecamere non collegate alla centrale operativa del corpo) per un periodo non superiore a 72 ore successive alla rilevazione, fatte salve speciali esigenze di sicurezza urbana e sicurezza pubblica.
- 2. In osservanza degli articoli 32 e 35 del GDPR e 23 e 25 della direttiva polizia, il Comune redige uno o più appositi atti di valutazione dei rischi e di valutazione di impatto sulla protezione dei dati ed adotta le misure in esse previste.
 - 3. Il Comune ha adottato una specifica procedura per la gestione degli incidenti di sicurezza/data breach che garantisce il rispetto delle disposizioni del GDPR e la notifica all'Autorità Garante per la Protezione dei dati personali in caso di violazioni di dati personali.

Art. 7 – Modalità di raccolta dei dati

- 1. I dati personali sono raccolti attraverso riprese video e captazione di immagini effettuate da sistemi di telecamere installate in luoghi pubblici ed aperti al pubblico nonché in immobili di proprietà comunale, ubicati nel territorio di competenza.
- 2. Le telecamere di cui al precedente comma, se finalizzate alla tutela della sicurezza urbana, consentono riprese video anche con utilizzo di algoritmi, possono essere dotate di brandeggio e di zoom ottico e sono collegate alla centrale operativa del Comando di Polizia Municipale, che potrà, esclusivamente per il perseguimento dei fini istituzionali, eventualmente digitalizzare o indicizzare le immagini.
- 3. Le immagini sono conservate per il periodo indicato all'articolo 6. Al termine del periodo stabilito il sistema di videoregistrazione provvede in automatico alla loro cancellazione, ove tecnicamente possibile, con modalità tali da rendere non più utilizzabili i dati cancellati.

Art. 8 - Diritti dell'interessato

- 1. In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, ha diritto, compatibilmente con i fini investigativi a tutela dell'ordine e sicurezza pubblica, prevenzione, accertamento o repressione di reati ai sensi della direttiva polizia:
 - a) di conoscere l'esistenza di trattamenti di dati che possono riguardarlo;
 - b) di essere informato sugli estremi identificativi del titolare e del designato al trattamento, oltre che sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali ed in generale di tutto quanto previsto *ex art.* 13 GDPR e art. 10 e ss. della direttiva polizia;
 - c) di ottenere:
 - la conferma dell'esistenza o meno di dati personali che lo riguardano;

- la trasmissione in forma intelligibile dei medesimi dati e della loro origine;
 - la cancellazione nei casi previsti dal GDPR qualora sussista uno dei motivi di cui all'art. 17 del GDPR, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- d) di opporsi, nei casi previsti dal GDPR, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'articolo 21 del GDPR. Il designato informerà l'interessato sull'esistenza o meno di motivi legittimi prevalenti;
- e) di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle ipotesi specificate all'art. 18 del GDPR. In tali casi i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico.
2. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
3. Le istanze sono presentate al titolare o al designato al trattamento.

Art. 9 – Accesso ai filmati.

1. Al di fuori dell'esercizio dei diritti dell'interessato, l'accesso ai filmati della videosorveglianza è consentito con le sole modalità previste dalla normativa vigente.
2. Ogni richiesta deve essere specifica, formulata per iscritto, motivata ed indirizzata al Comandante della Polizia Municipale entro 3 giorni dall'evento; decorso tale termine non è garantita la possibilità di evadere tempestivamente la richiesta entro il limite di conservazione dei filmati di cui all'art. 6, comma 1, lettera d) del presente regolamento.
3. L'accesso ai filmati della videosorveglianza comunale e dell'attività investigativa preventiva è consentito secondo le modalità previste dalla Legge n. 241/1990, fatta salva la diversa disciplina specifica di accesso ai documenti per motivi di giustizia.
4. Per finalità di indagine, l'Autorità giudiziaria e la Polizia giudiziaria possono richiedere ed acquisire copia delle immagini in formato digitale.
5. Nel caso di riprese relative ad incidenti stradali, anche in assenza di lesioni alle persone, copia delle riprese in formato digitale può essere richiesta ed acquisita dall'organo di polizia stradale che ha proceduto ai rilievi ed in capo al quale è l'istruttoria relativa all'incidente.
6. Nell'ambito delle investigazioni, il difensore, a norma dell'art. 391-quater c.p.p., può richiedere ed acquisire copia delle riprese in formato digitale previo pagamento delle relative spese individuate con apposita deliberazione di giunta comunale sulle tariffe di accesso ai documenti amministrativi.
7. La persona che ha la facoltà di proporre querela o che ha la facoltà o l'obbligo di presentare denuncia, nelle more di formalizzare denuncia o querela presso un ufficio di polizia, può

richiedere ai sensi dell'art. 18 del GDPR al Comando di Polizia Locale che i filmati siano conservati oltre i termini di legge, per essere messi a disposizione dell'organo di polizia procedente. L'interessato è tenuto a informare il Comando di Polizia Locale della data di presentazione della denuncia o querela, nonché l'organo di polizia presso il quale ha presentato denuncia o querela della richiesta di conservazione dei filmati per essere messi a disposizione della Polizia Giudiziaria entro un mese dalla presentazione della denuncia. Spetta all'organo di polizia procedente acquisire i filmati entro tale termine, decorso il quale i dati non saranno ulteriormente conservati.

8. In ogni caso di accoglimento delle richieste di cui ai commi precedenti, l'operatore autorizzato al trattamento dei dati deve annotare le operazioni eseguite al fine di acquisire i filmati e riversarli su supporto digitale, con lo scopo di garantire la genuinità dei dati stessi.
9. Possono essere divulgate immagini provenienti dagli impianti di videosorveglianza, previ anonimizzazione di ogni dato che consenta l'identificazione dei soggetti.

Art. 10 - Sicurezza dei dati

1. I dati personali oggetto di trattamento sono conservati presso la centrale di registrazione individuata, alla quale può accedere il solo personale autorizzato secondo istruzioni che devono essere impartite dal designato al trattamento dei dati.
2. In particolare, l'accesso agli ambienti in cui è ubicata una postazione di controllo è consentito solamente al personale autorizzato e per scopi connessi alle finalità previste, nonché al personale addetto alla manutenzione degli impianti, alla pulizia dei locali ed a occasionali motivi istituzionali.
3. Il designato impartisce idonee istruzioni atte ad evitare assunzioni o rilevamenti abusivi di dati da parte delle persone autorizzate all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali.
4. Il designato individua e nomina gli autorizzati in numero sufficiente a garantire la gestione del servizio di videosorveglianza.
5. La gestione e l'utilizzo dei sistemi di videosorveglianza aventi finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali è riservata agli organi di Polizia Municipale ed alle forze di polizia a competenza generale, aventi qualifica di ufficiali ed agenti di polizia giudiziaria ai sensi dell'art. 57 del codice di procedura penale.
6. Con l'atto di nomina, ai singoli autorizzati sono affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi in base alle differenti dislocazioni territoriali degli stessi.
7. In ogni caso, prima dell'utilizzo degli impianti, essi sono istruiti sul corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente regolamento.
8. Gli autorizzati al trattamento sono dotati di credenziali personali di autenticazione al sistema.
9. Il sistema deve essere fornito di log di accesso, che sono conservati per la durata di mesi sei.

Art. 11 – Cessazione del trattamento dei dati

1. In caso di cessazione, per qualsiasi causa, di un trattamento, i dati personali sono distrutti, ceduti o conservati secondo quanto previsto dal GDPR e dall'articolo 2 della direttiva polizia.

Art. 12 – Tutela amministrativa e giurisdizionale

1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli artt. 77 e seguenti del GDPR e dagli artt. 37 e seguenti della direttiva polizia.
2. In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 4-6 della Legge 7 agosto 1990, n. 241, è il designato al trattamento dei dati personali, così come individuato dal precedente art. 3.

Art. 13 – Disciplinare-programma

1. La giunta comunale, sulla base degli indirizzi e principi contenuti nel presente regolamento, con propria deliberazione, adotta e aggiorna il disciplinare-programma per l'utilizzo degli impianti di videosorveglianza.
2. Il disciplinare-programma può individuare anche qualsiasi altro dettaglio, specificazione, regolamentazione della videosorveglianza nel rispetto del presente regolamento.

Art. 14 – Norme finali

1. Dalla data di entrata in vigore del presente regolamento viene abrogato il regolamento per l'utilizzo di impianti di videosorveglianza del territorio approvato con deliberazione del Consiglio Comunale nr. ____ del ____ e deliberazione del Consiglio Comunale nr. ____ del ____ *[se presenti Regolamenti precedenti; altrimenti rimuovere questo punto]*.



COMUNE DI TREZZANO SUL NAVIGLIO

PROVINCIA DI MILANO

Via IV Novembre, 20090

Proposta N. 2026 / 2661

AREA POLIZIA LOCALE, PROTEZIONE CIVILE E SPORTELLLO UNICO ATTIVITA'
PRODUTTIVE

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

PARERE IN ORDINE ALLA REGOLARITA' TECNICA

Per i fini previsti dall'art. 49 del D. Lgs 18.08.2000 n° 267 e dell'art. 147 bis, si esprime
sulla proposta di deliberazione in oggetto parere *FAVOREVOLE* in merito alla regolarità
tecnica.

Lì, 28/08/2026

IL FUNZIONARIO
FESTA ANTONIO

(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)