Comune Dimaro Folgarida

Provincia di Trento

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 L'INNOVAZIONE DELLA SICUREZZA URBANA INTEGRATA

Elaborato

Rev .	0	Del	20.05.2022	Rapp:

Redatto da

Stefano Manzelli – Consulente Enti Locali e Forze Di Polizia
Giovanna Panucci – Avvocato e Dpo

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 possono utilizzare gli impianti per la tutela della sicurezza urbana riprendendo le strade e le piazze. La riforma sovranazionale sulla tutela dei dati personali entrata in vigore definitivamente nel 2018 ha rinnovato tutte le regole stabilendo in buona sostanza che spetta al titolare del trattamento (il comune) assumersi ogni responsabilità ed essere in grado di rendicontare le proprie scelte. 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. Questo provvedimento, specificamente dedicato alla tutela dei dati personali per i soggetti che svolgono indagini, compresa la polizia locale, deroga abbondantemente ad alcuni principi fondamentali del regolamento europeo sulla protezione dei dati. Oltre ad una necessaria conservazione allungata dei dati raccolti (anche alla luce del dl 139/2021) infatti, risultano decisamente affievoliti anche i diritti degli interessati che per esempio non potranno certo proporre l'opposizione al trattamento prevista ordinariamente dall'art. 21 del Gdpr. Senza un regolamento comunale che dia spazio alla direttiva Ue 2016/680 il rischio per i comuni è per esempio di non riuscire a gestire le richieste di esercizio dei diritti dell'interessato ai sensi degli artt. 12 e seguenti del Gdpr. Oppure di non poter attivare i collegamenti con polizia e carabinieri. Attenzione poi alla necessaria valutazione preventiva di impatto privacy. Un altro istituto poco conosciuto regolato sia dal Gdpr che dal d.lgs. 51/2018. Ogni moderno impianto di videosorveglianza urbana deve essere analizzato da un tecnico e un legale in modo da verificare preventivamente, dal punto di vista del cittadino, quali sono i rischi che emergono. Ovvero se il rischio che quelle immagini finiscano nel posto sbagliato è accettabile o meno. Senza questo certificato ogni impianto di videosorveglianza è potenzialmente a rischio di sanzione. Quindi ricapitolando per un comune che vuole attivare un nuovo sistema di videosorveglianza è necessario:

1) un regolamento aggiornato che regoli nel dettaglio tutti gli aspetti organizzativi;
2) un patto per la sicurezza per aprire alla corretta collaborazione interforze;
3) una obbligatoria di impatto privacy (dpia) che attesti il basso rischio dell'impianto;

Per effettuare questo tipo di regolamentazione è molto importante la collaborazione del responsabile della protezione dei dati con il titolare del trattamento (il comune ovvero il comandante della polizia locale) che non può mai sostituirsi ad eventuali consulenti esterni specializzati. Il dpo, infatti, dovrà validare la valutazione di impatto privacy (dpia), il regolamento e le altre attività amministrative conseguenti ma non potrà redigerle personalmente (per evidenti incompatibilità di ruolo tra controllore e controllato).
Due considerazioni importanti, infine, circa la necessità di dotarsi di un regolamento comunale aggiornato sulla videosorveglianza urbana e l'assoluta inadeguatezza nella complessa materia di eventuali indicazioni regionali. Con il parere rilasciato al Consiglio di Stato dal Garante per la protezione dei dati personali il 27 gennaio 2022 l'autorità ha evidenziato che non basta disporre della base giuridica del trattamento per essere in regola con la cattura di immagini. Serve regolare adeguatamente tutto il processo. E con il parere rilasciato dalla medesima Autorità alla Commissione Affari Costituzionali del Senato nella seduta n. 60 del 30 gennaio 2019 il Garante ha chiarito che nella materia della protezione dei dati lo Stato ha una competenza normativa esclusiva, come confermato dalla sentenza della Consulta n. 271/2005. Quindi le regioni sulla delicata materia non possono proprio intervenire.

1. INTRODUZIONE

Il Comune di Dimaro Folgarida ha la necessità di strutturare un progetto strategico di materia di videosorveglianza urbana integrata finalizzato alla regolarizzazione formale degli impianti di videosorveglianza presenti e futuri, in sincronia con la riforma della privacy (Regolamento UE 2016/679, D.lgs 196/2003 e successive modifiche), nel rispetto del D.L. 14/2017, convertito nella legge n. 48/2017 e della legge 205/2021.

Il presente progetto viene redatto sulla base della **delibera di Giunta n. 219 del 30/12/2021** avente per oggetto "affidamento del servizio di supporto strategico finalizzato alla realizzazione dei sistemi integrati di videosorveglianza e degli atti di regolamentazione e di condivisione dei dati, nonché alla redazione di un patto per la sicurezza urbana" da attivarsi attraverso:

- La realizzazione di un progetto strategico per l'inquadramento degli impianti di videosorveglianza, previo confronto con gli operatori, i tecnici, il DPO e il c.te.;
- Supporto alla regolarizzazione della privacy per la videosorveglianza con adozione di atti e di un nuovo regolamento per la tutela dei dati personali;
- Supporto alla redazione di un nuovo patto per la sicurezza;
- Supporto alla redazione delle convenzioni operative e 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** anche con eventuale collegamento Scntt per i veicoli rubati;
3) la **possibile sperimentazione di modelli tecnologici con uso di intelligenza artificiale**.

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 e stradale, ai sensi dell'art. 6 del dl 11/2009, 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 ex legge 205/2021), con titolarità del trattamento dei dati personali in capo al comune.

Per le altre forze di polizia: sarà opportuno 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.

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. Questo istituto, quindi, è una "componente sempre più significativa ed assorbente della categoria originaria e più generale della sicurezza pubblica". Il tema più affascinante resta quindi quello del corretto inquadramento giuridico della sicurezza urbana. Una specie di zona intermedia che non attiene né alla polizia amministrativa regionale né all'ordine e alla sicurezza pubblica in senso stretto formale, ma che legittima, ai sensi del dl 11/2009, la possibilità per i comuni di videosorvegliare le zone pubbliche e ad uso pubblico.

3. LE LINEE GENERALI DELL'INTEGRAZIONE

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. Oltre allo scambio informativo tra le forze di polizia locale e dello Stato, l'interconnessione delle sale operative e l'aggiornamento professionale integrato, uno dei filoni individuati dalle linee generali risulta quello della regolamentazione per l'utilizzo in comune tra polizia locale, polizia di Stato e carabinieri, con l'eventuale ausilio dei privati, dei sistemi di sicurezza tecnologica finalizzati al controllo delle aree e delle attività a rischio. Le linee generali specificano che in ogni caso saranno i prefetti a dover coordinare gli interventi di potenziamento e miglioramento degli impianti, in un'ottica di sicurezza integrata, avvalendosi del comitato provinciale per l'ordine e la sicurezza pubblica.

4. LE LINEE GUIDA E I PATTI *SINDACO - PREFETTO*

Le 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 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

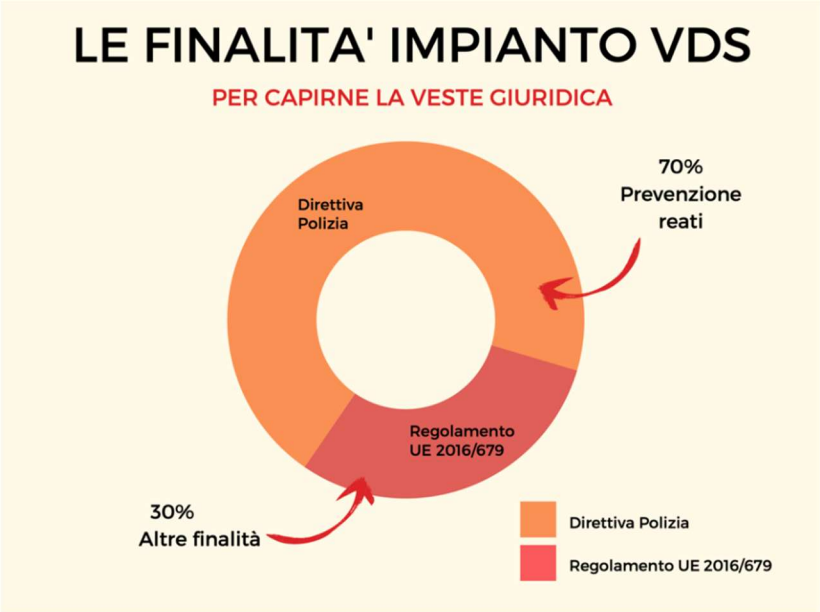
dell'utilizzo in comune degli apparati". Negli ultimi anni "è stata realizzata una copertura di videocamere sul territorio che ora si rende necessario ottimizzare e promuovere come sistemi integrati". Per il potenziamento dei rapporti di partenariato pubblico-privato le linee guida si soffermano sulle novità introdotte dal decreto sicurezza in materia di miglioramento degli impianti pubblici di videosorveglianza mediante l'introduzione di sistemi tecnologicamente avanzati dotati di software di analisi video in grado di allertare gli organi di controllo in tempo reale. La norma incentiva questa tipologia di installazioni moderne che, per essere effettivamente destinate ad un uso integrato di polizia, dovranno avere determinati requisiti ed essere approvati dalla prefettura.

5. 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.



6. PRIVATI E VIDEOSORVEGLIANZA

La partecipazione dei soggetti privati al potenziamento degli impianti di videosorveglianza è una pratica già ampiamente sperimentata da alcuni Comuni che hanno ammesso questa attività nel regolamento sulla videosorveglianza. In pratica il cittadino, l'associazione o l'operatore economico acquistano tecnologie e telecamere utili a migliorare gli impianti comunali (nella zona di interesse) e li mettono a completa disposizione del primo cittadino. Pur non potendo avere accesso diretto alle immagini, il miglioramento della sicurezza per l'area videosorvegliata è evidente e progressivo. La legge n. 48/2017 ne ha dato atto, ammettendo specifiche agevolazioni fiscali per chi investe in sicurezza urbana. Ma dovrà trattarsi di impianti moderni dotati di software di analisi video per il monitoraggio attivo con invio di segnali di allarme alle centrali delle forze di polizia o di istituti di vigilanza convenzionati, previa idonea e preventiva valutazione dell'impatto privacy. Per mettere in osservazione questi ambiti pubblici il dl 14/2017 richiede però alcuni importanti passaggi formali. Intanto il regolamento comunale dovrà disciplinare questa opportunità prevedendo specifici benefici fiscali in termini di Imu e Tasi. Chi investirà in tecnologie per la sicurezza della città dovrà infatti essere incentivato con l'applicazione di detrazioni dell'imposta municipale propria e del tributo per i servizi indivisibili.

7. 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.

8. IMPIANTI LETTURA TARGHE E SCNTT

Alla luce del dl 14/2017 e dopo lo stop all'accesso massivo alla banca dati dei veicoli rubati disponibile sul web, l'unico modo 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.

9. 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 205/2021in vigore dall'8 dicembre 2021. Pur applicandosi anche agli impianti di videosorveglianza cittadina, specificava 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 dall'art. 9, commi 9, 10, 11 del dl 139/2021 convertito nella legge 205/202, fino al 31 dicembre 2023 è stata di fatto vietata in Italia l'installazione e l'utilizzazione dei sistemi di riconoscimento facciale. Ma questo divieto ai sensi del successivo comma 12 non si applica ai trattamenti effettuati dalle autorità

competenti ai fini di prevenzione e repressione dei reati, previo parere favorevole del Garante alla necessaria valutazione obbligatoria di impatto (Dpia).

10. 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.

11. BODYCAM CON RISERVA IN CERTE CONDIZIONI

Nel caso di servizi di ordine pubblico le forze di polizia potranno utilizzare dispositivi di videoripresa portatili ma facendo particolare attenzione al corretto trattamento dei dati personali. In ogni caso le telecamere che riprendono manifestazioni pubbliche generano sempre un trattamento di dati ad elevato rischio che richiede una valutazione preventiva dell'autorità. Lo ha evidenziato il Garante per la protezione dei dati personali con il parere n. 9690902 del 22 luglio 2021. I carabinieri e la polizia hanno deciso di attivare delle telecamere indossabili da mettere a disposizione degli operatori in caso di servizi critici di ordine e sicurezza pubblica. Per questo motivo hanno realizzato una valutazione di impatto sulla privacy del progetto che poi hanno inviato al garante ai sensi dell'art. 24 del dlgs 51/2018. L'autorità ha dato il via libera di massima all'iniziativa con una serie di raccomandazioni che si sono trasformate in indicazioni operative con la circolare del Ministero dell'interno del 18 gennaio 2022 (che rappresenta un utile caposaldo anche per la regolamentazione delle bodycam in uso alla polizia locale). Finalmente gli strumenti potranno essere utilizzati ma nello scrupoloso rispetto delle linee guida diramate dal Viminale. Le videocamere individuali vengono assegnate all'operatore volta per volta e non sono configurabili dallo stesso. In pratica le bodycam possono solo essere attivate quando vi è necessità di registrare eventi e salvo casi eccezionali nessuno potrà immediatamente avere accesso ai filmati catturati dai dispositivi. A fine turno le bodycam verranno spente definitivamente e i filmati esportati automaticamente dalla memoria locale nel momento del deposito del dispositivo sulla docking station. Le immagini verranno quindi conservate nel server del Viminale per un periodo massimo di 6 mesi, salvo ulteriori esigenze investigative da verificare volta per volta. Sulle questioni privacy la circolare è molto chiara. Il titolare del trattamento è il ministero dell'interno inteso nel complesso delle sue articolazioni esercenti in quota parte la specifica funzione. I filmati catturati non costituiscono un dato biometrico

perché normalmente non vengono impiegati software per il riconoscimento facciale. Gli autorizzati al trattamento sono tutti gli attori formalmente individuati nella scala gerarchica delle singole organizzazioni. La base giuridica del trattamento è ampiamente reperibile nelle diverse disposizioni normative che attribuiscono agli organi di polizia potere di intervento e di indagine in materia di ordine pubblico e polizia giudiziaria, conclude la circolare.

12. 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 inidonei 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 rientrino 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 quando 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.

13. 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. In particolare, le lettere c) e d) dell'articolo in questione consentono la limitazione dei diritti dell'interessato al fine di salvaguardare, rispettivamente, la sicurezza pubblica e l'attività di prevenzione, accertamento e repressione dei reati. Per quanto attiene le misure di sicurezza, queste subiscono una importante rivisitazione: come già detto, nell'ottica di una maggiore responsabilizzazione del titolare e del responsabile del trattamento, saranno proprio questi a valutare i rischi specifici e ad adottare idonee misure a protezione del sistema e dei dati. Ciò implica che le misure indicate dall'art. 32 del regolamento non siano da intendersi esemplificative, ed anzi non risultano nemmeno applicabili le misure minime previste dal codice privacy. 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.

14. 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.

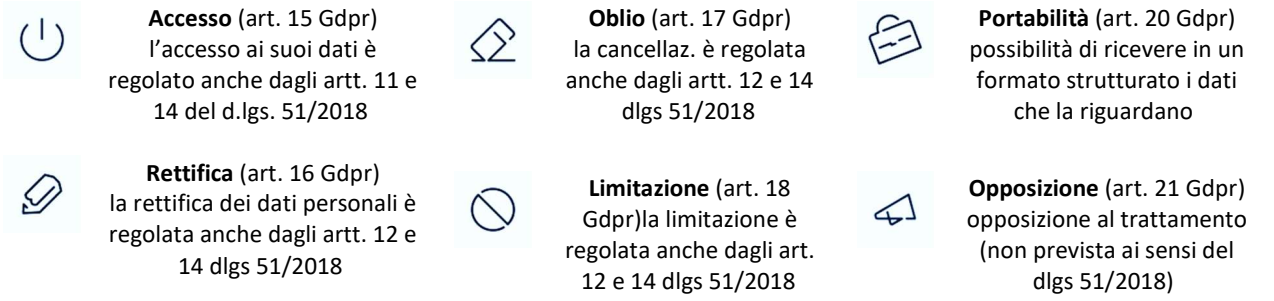
15. LE FAQ DEL GARANTE SULLA VIDEOSORVEGLIANZA GDPR

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.

16. I DIRITTI DEGLI INTERESSATI SUI DATI IN CONCRETO

Videosorveglianza e diritto alla riservatezza sono due materie che necessitano di apposite regolamentazioni al fine di poter convivere reciprocamente l'una accanto all'altra. Infatti, se da un lato il cittadino ha diritto alla protezione dei dati che lo riguardano dall'altra l'autorità ha il dovere di contribuire al potenziamento della sicurezza delle città. Il bilanciamento di queste finalità è essenziale allo scopo di delineare il quadro dei diritti che possono essere esercitati e stabilire i limiti affinché tutti i soggetti possano essere parimenti tutelati. 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 amministrativi (i filmati), 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.** 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.

Impianti di videosorveglianza urbana e diritti degli interessati sulla tutela dei dati



17. LA VALUTAZIONE OBBLIGATORIA DI IMPATTO

L'attività di videosorveglianza urbana prevede l'uso di tecnologie all'avanguardia e, considerata la natura, l'oggetto, il contesto e le finalità di trattamento, presenta sicuramente un elevato rischio per i diritti e le libertà dei cittadini, per questo motivo, ai sensi dell'art. 35 par. 3 lett. c). del regolamento Ue 2016/679, e art. 23 del D.lgs. 51/2018, essa risulta soggetta all'obbligo di valutazione d'impatto sulla protezione dei dati. Tale valutazione, di natura obbligatoria, prevista dall'art. 15 del regolamento Ue 2016/679 e dall'art. 23 del D.lgs. 51/2018, ha la funzione di studiare il grado di rischio del trattamento che si vuole compiere,

esaminando le aree critiche, il profilo di tutti i soggetti coinvolti, gli effetti e le conseguenze del trattamento dei dati e la valutazione dei rischi collegati, arrivando quindi alla stesura di un piano di mitigazione di questi ultimi. Per “rischio” si intende uno scenario descrittivo di un evento e delle relative conseguenze stimate in termini di gravità e probabilità, che possono essere: perdita, rilevazione e accesso non autorizzato ai dati. I rischi citati posso provocare ingenti danni ai diritti e alle libertà dell’individuo, perciò devono essere valutati con cura e limitati attraverso l’applicazione di misure tecnico-organizzative da parte del titolare o, nei casi più complessi, dall’autorità competente. Comune e forze di polizia devono adottare minuziosamente ogni tipo di misura per evitare il rischio di un trattamento erroneo dei dati. Data la natura pericolosa del rischio, è inevitabile che la Dpia vada condotta per ogni impianto di videosorveglianza poiché è necessaria l’individuazione delle contromisure utili per diminuire il rischio relativo alla violazione della privacy del soggetto fisico, con lo scopo di rendere il trattamento accettabile dal lato della tutela e dalla sicurezza. Il suo fine è, infatti, quello di valutare il trattamento e assicurare ai soggetti che transitano sotto gli impianti di videosorveglianza l’assenza di eventi dannosi derivanti dall’uso sbagliato dell’impianto e/o del trattamento dei dati. Ridurre quasi a zero il rischio di malfunzionamento o di uso non consono delle videocamere è il primo passo per mettere al centro della disciplina l’interessato, quindi rendere sicura l’operazione dell’Autorità ed instaurare un rapporto di fiducia. A tal riguardo, la Dpia è uno strumento estremamente importante in termini di responsabilizzazione: da un lato aiuta il titolare a rispettare le prescrizioni del Regolamento Ue 2016/679 e della direttiva polizia, dall’altro, attraverso una prima valutazione e il riesame costante di essa nel corso del tempo, garantisce la più ampia protezione del cittadino e dei suoi diritti. L’obbligo di condurre una Dpia, in circostanze come questa, deve essere collocato nel contesto del più generale obbligo imposto ai titolari di trattamento di gestire correttamente i rischi connessi al trattamento di dati personali. A tal riguardo, la complessa e precisa valutazione dei rischi in cui può incorrere il soggetto deve essere realizzata attraverso l’affiancamento del titolare a soggetti competenti in ambito tecnico informatico, organizzativo, legale e protezione dati. Solo attraverso un’attività scrupolosa di valutazione si potrà arrivare ad una riduzione del rischio per i dati dell’individuo e, nella remota e malaugurata ipotesi in cui accada un evento dannoso, si avrà la facoltà di provare che tutte le misure atte ad evitare quella situazione era comunque state adottate. Riducendo il rischio del cittadino e uniformandosi alla disciplina si può quindi arrivare a creare un procedimento sempre più sicuro di trattamento dei dati.

18. LA NECESSITÀ DI FORMALIZZARE ACCORDI CON LE PREFETTURE

Tutti gli impianti di videosorveglianza comunale installati per finalità di sicurezza urbana ovvero di tutela dell’ordine pubblico e per finalità di accertamento e prevenzione dei reati possono essere visionati dagli organi di indagine. Lo stesso vale per la visione dei filmati di telecamere private che possono essere indirizzate anche verso le aree pubbliche previo accordo vincolante con l’amministrazione comunale. A tal fine il Garante per la protezione dei dati personali con il parere n. 30246/2016 indirizzato al comune di Olgiate Olona, ha messo in luce un aspetto fondamentale, quello che la finalità del trattamento è strettamente correlata alla titolarità; qualora la finalità sia la tutela della sicurezza urbana la titolarità compete al comune. Con la sottoscrizione dei patti per la sicurezza tra il prefetto e il sindaco si pone la questione di individuare, in base alle diverse finalità perseguite a chi spetti la titolarità, se essa sia da attribuire al comune o se rientri nell’articolo 17 del D.lgs. 51/2018 che prevede che due o più titolari del trattamento che determinano congiuntamente le finalità i mezzi del trattamento sono contitolari. L’inquadramento in un senso o nell’altro è fondamentale per delimitare gli ambiti delle rispettive responsabilità e soprattutto, per consentire ai titolari stessi di designare i responsabili del trattamento tenuti ad effettuare il trattamento per loro conto. I contitolari determinano mediante un accordo che può rivestire le forme dell’accordo tra pubbliche amministrazioni ai sensi dell’articolo 15 della Legge

241/1990, gli ambiti delle rispettive responsabilità per l'osservanza delle norme di cui al presente decreto e per designare il punto di contatto per gli interessati. L'accordo di contitolarità è lo strumento che meglio consente di regolamentare dettagliatamente i rapporti tra i diversi titolari in relazione alle finalità sottese all'uso di un impianto di videosorveglianza soprattutto se dotato di un sistema di lettura targa e eventuale collegamento al ced del dipartimento della polizia di Stato per la consultazione dei dati e delle informazioni relative ai veicoli rubati. Diverse sono le autorità a presidio delle finalità: sindaco per la sicurezza urbana, prefetto per la sicurezza pubblica, questura per l'ordine pubblico, procura della Repubblica per la prevenzione, indagine, accertamento e perseguimento di reati. Gli accordi di contitolarità cominciano a trovare spazio all'interno di progetti di sicurezza urbana integrata, ma la strada è ancora costellata di tipologie di atti dei più disparati sia dal punto di vista della struttura che dei contenuti. E recenti linee guida del comitato europeo per la protezione dei dati n. 7/2020 sembrano rivalutare anche la possibilità di gestione comune della stessa tecnologia tra titolari autonomi.

19. IL REGISTRO DEI TRATTAMENTI E LE INFORMATIVE

Un progetto di definizione strategica e normativa deve tenere necessariamente in considerazione anche l'allineamento del registro dei trattamenti alle scelte organizzative e strutturali intraprese, soprattutto con riferimento alle informative di primo e secondo livello. Il registro dei trattamenti, previsto all'art. 30 del GDPR, rappresenta, di fatto, un importantissimo strumento di accountability, riportando in veste grafica i dati già inseriti nella modulistica privacy di supporto. Pertanto, è fondamentale che il contenuto delle informative sia coerentemente riprodotto nel registro dei trattamenti dell'ente, il quale dovrà indicare, ad esempio, le finalità del trattamento, la durata della conservazione dei dati, i soggetti autorizzati, le politiche di accesso, i responsabili esterni e le misure di sicurezza implementate. Di seguito un esempio di informativa di primo livello.

20. LE LINEE GUIDA SULLA TITOLARITÀ E CONTITOLARITÀ

Il comitato europeo per la protezione dei dati ha diramato nel mese di settembre 2020 un importante strumento che può aiutare l'interprete nella corretta individuazione dei "ruoli privacy" in materia di videosorveglianza urbana integrata. Si tratta delle linee guida sui concetti di titolare e responsabile del trattamento aggiornati alla riforma europea della privacy. Spunti importanti possono essere ricavati in materia di contitolarità. In particolare, si segnala il paragrafo 3.2.2.1 che allarga l'ipotesi di contitolarità anche agli enti che non

perseguono esattamente le stesse finalità purché le stesse siano convergenti ma con impatto tangibile e inestricabile. Queste nuove complesse indicazioni potrebbero aiutare l'interprete e i responsabili della protezione dei dati a comprendere meglio come organizzare gli accordi tra polizia locale e forze di polizia dello Stato in materia di utilizzo condiviso della stessa infrastruttura. Nel frattempo, però meglio sempre tenere anche presente il paragrafo 4.6 e 5 del provvedimento generale del Garante italiano 2010 in materia di videosorveglianza laddove lo stesso evidenzia che i titolari autonomi del trattamento possono utilizzare le medesime infrastrutture tecnologiche senza troppe formalità. Ma in mancanza di indicazioni dell'Autorità sull'attualità di questo provvedimento, ormai datato, ogni ipotesi resta teoricamente possibile: polizia locale e altre forze di polizia titolari autonomi che usano la stessa infrastruttura oppure contitolari con finalità diverse ma convergenti. Alla luce delle linee guida 7/2020 le ipotesi di autonoma titolarità risultano ancora possibili. Quindi la nuova stagione degli accordi interforze sembra orientata alla contitolarità ma non per tutti e quindi il processo di revisione e aggiornamento degli accordi sarà necessariamente lungo e complesso.

21. GESTIONE CONCRETA DELLA PRIVACY/1: TITOLARITÀ' AUTONOMA

Come abbiamo visto, si ritiene opportuno impostare il trattamento dei dati personali nel rispetto della disciplina introdotta dal d.lgs. 51/2018 oltre che al Gdpr. Questa importante strategia avrà necessariamente effetti anche nell'organizzazione interforze dei sistemi ed in particolare nell'architettura generale e complessiva del presente progetto. 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 titolari autonomi sotto l'egida, comunque, del d.lgs. 51/2018. Per formalizzare un'attività interforze in questo caso occorrerà regolare un rapporto dove in pratica si evincerà che il comune persegue le finalità di sicurezza urbana con i propri strumenti di videosorveglianza come titolare autonomo. La prefettura dal canto suo persegue finalità di ordine e sicurezza pubblica e per raggiungere queste finalità potrà ritenere che il mezzo migliore sia l'utilizzo del sistema di videosorveglianza comunale. Per tale motivo, quindi, deve essere considerata titolare autonomo. 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 prefettura con un accordo che metta in evidenza come il comune diventi di fatto il gestore di un

impianto di videosorveglianza interforze cui accede in sicurezza ed autonomia anche la prefettura (e quindi tutte le forze di polizia dello Stato), 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. Si tratta di comprendere come mettere in sicurezza i sistemi e in questo senso pare che la scelta di server ridondanti sia quello più semplice.

22. GESTIONE CONCRETA DELLA PRIVACY/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". Ed è proprio quello che è successo a Livorno, dove il comune ha recepito la richiesta dell'Utg di potenziare i sistemi di videosorveglianza per finalità anche di sicurezza pubblica e all'esito dell'installazione, prima di utilizzare i nuovi dispositivi, ha richiesto di formalizzare l'uso di queste installazioni con un accordo di contitolarità sul trattamento dei dati personali.

23. GESTIONE CONCRETA DELLA PRIVACY/3: NOMINA DI DESIGNATI

La terza ipotesi 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. Secondo il disposto dell'articolo, infatti, *il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.* L'ente pubblico può, quindi, redigere delle specifiche deleghe singole o per tipologie di autorizzati/designati, delimitando l'ambito del trattamento e consentendo, in ottica di "accountability", di dare seguito agli adempimenti organizzativi interni alla propria struttura per essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR. La designazione avverrà formalmente attraverso la sottoscrizione da parte del comune e delle forze di polizia di un accordo (specificamente preceduto da un patto per la sicurezza sottoscritto in prefettura), con la conseguente attribuzione di specifici compiti e funzioni sul trattamento dei dati personali nei limiti e nelle modalità impartite dal titolare di trattamento. Ai designati speciali si estendono tutti gli obblighi in capo al titolare del trattamento e nello specifico il principio di trasparenza, limitazione e minimizzazione del trattamento e gli obblighi di cui all'art. 5 D.lgs 51/2018. A livello logistico/operativo, le forze di polizia dello Stato avranno quindi la possibilità di **accedere**, per il periodo di validità della nomina, ai sistemi di videosorveglianza attraverso autorizzazioni determinate, personali con credenziali di accesso che verranno dettagliate e verticalizzare caso per caso. Attraverso questo modello di gestione, seppur ibrido, il titolare ottempera al principio di "responsabilizzazione" che attribuisce allo stesso il compito di assicurare ed essere in grado di comprovare sempre e comunque il rispetto dei principi applicabili al trattamento dei dati personali e di adottare quelle misure che vengano valutate a ciò più idonee ed opportune a seconda del caso di specie e della realtà organizzativa di riferimento, riducendo il rischio al minimo.

24. L'AFFRETTATA RIFORMA 2022 DELLA PRIVACY (LEGGE 205/2021)

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 potrà 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. Qualche amministratore temerario per finalità tipiche del comune come, per esempio, la tutela della sicurezza stradale e della pirateria potrebbe, attraverso l'assunzione di atti amministrativi innovativi, pensare addirittura di "riesumare" il riconoscimento facciale mediante dispositivi di video-audio ripresa che, sebbene messi "al bando" sino a fine dicembre 2023, potrebbero essere utilizzati per esigenze investigative, previo parere dell'Autorità. Oppure qualche primo cittadino creativo potrebbe decidere di mettere in chiaro informazioni, filmati e dati personali per millantate esigenze di pubblico interesse come, per esempio, divulgare sulla rete le immagini degli automobilisti particolarmente negligenti. Insomma, senza una indicazione centrale che peraltro dovrà verificare anche il reale perimetro di sostenibilità tecnico giuridica dell'intera riforma affrettata della privacy che a

nostro parere rischia numerose censure di inadeguatezza non solo costituzionale, non è opportuno discostarsi dall'impianto attuale proposto fin qui in materia di corretto trattamento dei dati personali e impianti di videosorveglianza urbana integrata. **Gli unici suggerimenti operativi, in attesa di eventuali indicazioni centrali, possono riguardare innanzitutto il potenziamento della base giuridica per la conservazione allargata fino ad almeno 90 giorni dei transiti targhe catturati con gli ocr.** 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. **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**.

25. IL CONFRONTO CON GLI ATTORI

Nel corso della videochiamata effettuata il **23 febbraio 2022** sono stati identificati gli aspetti rilevanti del sistema di videosorveglianza del Comune Dimaro Folgarida e la sua organizzazione strategica in itinere. Innanzitutto, qualche considerazione di contesto. Il sistema di videosorveglianza è condiviso fra i Comuni della Val di sole, a cui Dimaro Folgarida appartiene. La Comunità della Valle di Sole è un ente intermedio senza riconoscimento costituzionale che ha individuato nel Comune Dimaro Folgarida l'ente capofila nella gestione di sistemi di videosorveglianza. L'organizzazione del servizio di videosorveglianza dei numerosi comuni dell'area fa riferimento, tecnicamente, al Comune di Dimaro Folgarida. La proprietà dell'impianto rimane della Comunità della Valle che lo ha dato in comodato d'uso gratuito ai singoli comuni. Alla luce della complessità organizzativa del territorio si è concordato di strutturare un modello di regolamento comunale da fare adottare a tutti i comuni che faranno rispettivamente riferimento a Dimaro Folgarida. In questa realtà sarà cruciale la valorizzazione della centrale operativa della polizia locale che fungerà da raccordo tra i comuni contigui in linea con la convenzione ad oggi in vigore. Lasciando quindi i singoli comuni titolari del trattamento ma regolando in sicurezza l'uso condiviso delle immagini che arrivano nella centrale operativa condivisa. Dal punto di vista tecnico l'impianto comunale è moderno ed efficace e non necessità di particolari interventi di miglioramento. L'impianto è, peraltro, molto razionale. Sono infatti presenti n. 20 telecamere di contesto. Non viene fatto uso di bodycam o droni. Sono presenti n. 21 telecamere di lettura targhe con sistemi OCR, modello Bosch. Non viene fatto uso di fototrappole per il controllo dei rifiuti. La gestione tecnica del sistema di videosorveglianza è affidata ad una ditta esterna che si occupa della manutenzione dei server e dei sistemi. Si tratterà di regolamentare bene i rapporti con i responsabili esterni del servizio e di verificare se la ditta è stata nominata anche amministratore di sistema. Il rapporto interforze non è stato perfezionato. Manca infatti un patto per la sicurezza che è necessario per dare stabilità ai rapporti. Vi è, comunque la volontà di traguardare la sottoscrizione di un nuovo accordo formale fra polizia e carabinieri che consenta a questi ultimi di accedere alle immagini in maniera totalmente indipendente e soprattutto agevole. Questo accordo rappresenterà uno strumento molto importante che l'amministrazione intende raggiungere nel breve periodo. Appena i comuni avranno recepito lo stesso modello di regolamento sarà possibile proporre un patto per la sicurezza analogo che per tutti gli enti, finalizzato ad agevolare l'accesso stabile di tutte le forze di polizia innanzitutto al sistema centralizzato di videosorveglianza. La soluzione formale suggerita è quella della nomina delle forze di polizia dello Stato come *designati speciali al trattamento*, una soluzione semplificata di concreto interesse operativo. Il disciplinare programma che ogni amministrazione comunale andrà ad adottare potrà

perfezionare e personalizzare meglio le singole esigenze locali. Mentre la valutazione di impatto privacy in corso di realizzazione per conto del Comune di Dimaro Folgarida fornirà adeguata e necessaria tutela al trattamento dei dati personali.

26. 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 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 il Comune di Dimaro Folgarida, ente capofila, ha una forte consapevolezza dell'importanza di traguardare interventi strutturati di sicurezza urbana integrata. È attualmente presente un parco tecnologico moderno e adeguato che potrà essere nel corso del tempo ulteriormente potenziato, nel rispetto delle diverse prerogative degli operatori di polizia coinvolti. Ora si tratta di procedere a formalizzare tutti gli atti e le attività formative ed organizzative conseguenti al fine di perfezionare l'attività anche con una necessaria valutazione di impatto privacy (dpia). Dopo aver approvato un nuovo regolamento aggiornato sulla vds, anche ai sensi della legge n. 205/2021 sarà opportuno proporre alla Prefettura la condivisione del presente progetto strategico per ammettere, previa necessaria sottoscrizione di un patto per la sicurezza, l'avvio di un robusto percorso interforze finalizzato alla creazione di un comprensorio interamente controllato con varchi lettura targhe condivisi tra forze di polizia locale e dello Stato.

Faenza, 20 maggio 2022

Allegati:

1. **Traccia patto per la sicurezza**
2. **Traccia regolamento comunale sulla videosorveglianza**
3. **Traccia possibile accordo sintetico tra forze di polizia locale e dello Stato**
4. **Traccia matrice registro dei trattamenti (estratto trattamenti da vds)**

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