COMUNE DI VALFENERA

VALUTAZIONE DI IMPATTO

ART. 35 DEL REGOLAMENTO GENERALE
SULLA PROTEZIONE DEI DATI (G.D.P.R.)
Regolamento (UE) 2016/679 del Parlamento Europeo
e del Consiglio del 27/04/2016

SISTEMA DI VIDEOSORVEGLIANZA

INDICE

1. RELAZIONE INTRODUTTIVA

1.1. PREMESSA

Il presente documento (valutazione d'impatto sulla protezione dei dati) viene redatto in ottemperanza a quanto previsto dall'art. 35 del Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 che dispone che quando un tipo di trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

La valutazione di impatto (o D.P.I.A. Data Protection Impact Assessment) è un processo volto a descrivere il trattamento, valutarne la necessità e la proporzionalità e a gestire gli eventuali rischi per i diritti e le libertà delle persone derivanti dal trattamento e costituisce lo strumento principale tramite il quale il titolare effettua l'analisi dei rischi derivanti dai trattamenti posti in essere. Il titolare, sviluppando una valutazione preventiva delle eventuali conseguenze del trattamento dei dati personali sulle libertà e i diritti degli interessati calcolandone su di essi il livello di impatto.

La norma invocata prevede che il titolare del trattamento, allorquando svolga una valutazione d'impatto sulla protezione dei dati, si consulti con il responsabile della protezione dei dati (DPO).

La valutazione d'impatto sulla protezione dei dati è richiesta in particolare quando sono effettuate le seguenti tipologie di trattamenti:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati;
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il Considerando 91 del Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 circoscrive il concetto di "larga scala", fondamentale per l'interpretazione della disposizione, e definisce i trattamenti su larga scala come quelli che "(…) che mirano al trattamento di una notevole quantità di dati personali (…) che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato".

L'art 35, comma 5, del Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 prevede che le Autorità

nazionali possano redigere un elenco pubblico di tipologie di trattamenti per i quali si rende necessaria la valutazione di impatto. L'Autorità Garante nazionale ha pubblicato tale elenco con Provvedimento 11/10/2018, vincolante ma non esaustivo, fermo restando l'obbligo di adottare una valutazione d'impatto sulla protezione dei dati laddove ricorrano i criteri individuati dal documento denominato Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - Versione 2.0 adottate il 29/01/2020, elenco comprende "trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati (…).

La valutazione contiene almeno:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al G.D.P.R., tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

L'Autorità aveva a suo tempo già ricompreso nelle fattispecie da assoggettare alla verifica preliminare (procedura attualmente non prevista a seguito dell'introduzione della disciplina sulla valutazione di impatto ad opera G.D.P.R.) i sistemi di raccolta delle immagini associate a dati biometrici (in particolare quelli che impiegano un software che consente il riconoscimento di una persona tramite incrocio o confronto delle immagini rilevate con dati biometrici dell'individuo o con una campionatura di persone precedentemente costituita) in quanto l'uso generalizzato e incontrollato di tale tipologia di dati può comportare il concreto rischio del verificarsi di un pregiudizio rilevante per l'interessato. Medesimo inquadramento era stato riservato anche ai sistemi integrati di videosorveglianza ed ai cd. "sistemi intelligenti", in grado di rilevare ed analizzare automaticamente situazioni o comportamenti e definirli coma anomali. Tali ultimi sistemi erano da considerarsi eccedenti rispetto alla normale attività di videosorveglianza, in quanto passibili di determinare effetti particolarmente invasivi sulla sfera di autodeterminazione dell'interessato e, conseguentemente, sul suo comportamento. Il relativo utilizzo risultava comunque giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati, da verificare caso per caso sul piano della conformità ai principi di necessità, proporzionalità, finalità e correttezza dettati dal vigente **"**Codice in materia di protezione dei dati personali".

La valutazione di impatto, pur in assenza dell'interfaccia autorizzativa preliminare con l'Autorità implica in ogni caso l'analisi e la descrizione delle aree critiche da esaminare, del profilo di tutti i soggetti coinvolti, gli effetti e le conseguenze del trattamento dei dati, una valutazione dei rischi collegati, e quindi la stesura di un piano di mitigazione dei rischi

Il progetto relativo alla realizzazione ed attivazione del sistema di videosorveglianza del Comune di Valfenera, anche nel caso in cui fosse implementato con l'introduzione dei cd. "sistemi intelligenti" (videoanalisi) e degli apparati per le cd "plurime finalità" consente il trattamento di dati personali nell'ambito di una attività di videosorveglianza nel rispetto delle misure e degli accorgimenti prescritti dalla medesima Autorità Garante (Provvedimento in materia di videosorveglianza del 08/04/2010 - G.U. n. 99 del 29/04/2010).

La realizzazione/implementazione ed attivazione del sistema di videosorveglianza del Comune di Valfenera ricade nell'ipotesi di sorveglianza sistematica su larga scala, così come nella fattispecie prevista dal G.D.P.R., sostanzialmente sovrapponibile alla verifica preliminare di cui all'allora vigente art. 17 del D.Lgs 196/2003 "Codice in materia di protezione dei dati personali", che subordina l'operatività del trattamento ad una consultazione dell'Autorità di Controllo solo qualora la valutazione di impatto dimostri un rischio elevato gravante sul trattamento previsto in assenza di idonee misure di mitigazione.

Il presente documento si prefigge lo scopo di fornire al titolare del trattamento tutti gli elementi necessari per poter valutare la conformità del trattamento dei dati personali ai principi fissati dal G.D.P.R.

Il Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 prevede che il titolare del trattamento ponga in essere misure adeguate per garantire ed essere in grado di dimostrare il rispetto di detto regolamento, tenendo conto, tra l'altro, dei "rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche". L'obbligo per i titolari del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati va inteso nel contesto dell'obbligo generale, cui gli stessi sonosoggetti, di gestire adeguatamente i rischi presentati dal trattamento di dati personali.

Un "rischio" è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. La "gestione dei rischi", invece, può essere definita come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.

Il richiamato art. 35 del Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 fa riferimento al possibile rischio elevato "per i diritti e le libertà delle persone fisiche". Come indicato nella dichiarazione del Gruppo di Lavoro Articolo 29 sulla protezione dei dati sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati, il riferimento a "diritti e libertà" degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.

Le linee guida in materia di valutazione d'impatto sulla protezione dei dati (Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - Versione 2.0 adottate il 29/01/2020) forniscono indicazioni ed esempi più dettagliati relativi alla videosorveglianza, con particolare

riferimento alle finalità tipiche della videosorveglianza (protezione delle persone e dei beni, individuazione, prevenzione e controllo di reati, raccolta di elementi di prova e identificazione di soggetti). L'esito della valutazione d'impatto sulla protezione dei dati deve determinare la scelta del titolare del trattamento in merito alle misure di protezione dei dati da introdurre o implementate. È inoltre importante ricordare che, ove i risultati della valutazione d'impatto sulla protezione dei dati indichino che il trattamento comporterebbe un rischio elevato nonostante le misure di sicurezza pianificate dal titolare, occorrerà consultare l'Autorità Garante prima di procedere al trattamento. Le disposizioni in materia di consultazioni preventive sono contenute nell'art. 36 del Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016.

Una valutazione d'impatto sulla protezione dei dati può riguardare una singola operazione di trattamento dei dati. Tuttavia, l'art. 35, paragrafo 1, indica che "una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi". Il Considerando 92 aggiunge che "vi sono circostanze in cui può essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che verta su un oggetto più ampio di un unico progetto, per esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata".

Si potrebbe ricorrere a una singola valutazione d'impatto sulla protezione dei dati nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. In effetti, le valutazioni d'impatto sulla protezione dei dati mirano a studiare sistematicamente nuove situazioni che potrebbero portare a rischi elevati per i diritti e le libertà delle persone fisiche e non è necessario realizzare una valutazione d'impatto sulla protezione dei dati nei casi (ad esempio operazioni di trattamento in un contesto specifico e per una finalità specifica) che sono già stati studiati. Questo potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità.

Qualora il trattamento coinvolga contitolari del trattamento, questi ultimi devono definire con precisione le rispettive competenze. La loro valutazione d'impatto sulla protezione dei dati deve stabilire quale parte sia competente per le varie misure volte a trattare i rischi e a proteggere i diritti e le libertà degli interessati. Ciascun titolare del trattamento deve esprimere le proprie esigenze e condividere informazioni utili senza compromettere eventuali segreti (ad esempio protezione di segreti aziendali, proprietà intellettuale, informazioni aziendali riservate) o divulgare vulnerabilità. Una valutazione d'impatto sulla protezione dei dati può essere altresì utile per valutare l'impatto sulla protezione dei dati di un prodotto tecnologico, ad esempio un dispositivo hardware o un software, qualora sia probabile che lo stesso venga utilizzato da titolari del trattamento distinti per svolgere tipologie diverse di trattamento. Ovviamente, il titolare del trattamento che utilizza detto prodotto resta soggetto all'obbligo di svolgere la propria valutazione d'impatto sulla protezione dei dati in relazione all'attuazione specifica, tuttavia tale

valutazione del titolare del trattamento può utilizzare le informazioni fornite da una valutazione analoga preparata dal fornitore del prodotto, se opportuno.

Rispetto ai trattamenti assoggettabili a valutazione di impatto il G.D.P.R. la ritiene necessaria qualora un trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche" e, per quanto pertinente, alla trattamento riconducibile al monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (art. 35, paragrafo 3, lettera c) . Questo tipo di monitoraggio è considerato critico in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico).

Marginalmente, ma in ogni caso nell'ambito generale della categoria di "monitoraggio sistematico" in stretto riferimento alla cd. "videoanalisi", è potenzialmente possibile il ricorrere della fattispecie relativa all'uso innovativo o all'applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici. In tal senso il Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 chiarisce che l'uso di una nuova tecnologia, definita "in conformità con il grado di conoscenze tecnologiche raggiunto" (Considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi.

L'obbligo di svolgere una valutazione d'impatto sulla protezione dei dati si applica alle operazioni di trattamento esistenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche e per le quali vi è stata una variazione dei rischi, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

Non è necessaria una valutazione d'impatto sulla protezione dei dati per i trattamenti che sono stati verificati da un'Autorità di controllo o dal responsabile della protezione dei dati, a norma dell'art. 20 della Direttiva 95/46/CE e che vengono eseguiti in maniera tale da fare sì che non si sia registrata alcuna variazione rispetto alla verifica precedente. In effetti, "(…) le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate" (considerando 171).

Al contrario, ciò significa che qualsiasi trattamento di dati le cui condizioni di attuazione (ambito di applicazione, finalità, dati personali raccolti, identità dei titolari del trattamento o dei destinatari,

periodo di conservazione dei dati, misure tecniche e organizzative, ...) sono mutate rispetto alla prima verifica effettuata dall'autorità di controllo o dal responsabile della protezione dei dati e che possono presentare un rischio elevato devono essere soggette a una valutazione d'impatto.

Inoltre, potrebbe essere richiesta una valutazione d'impatto sulla protezione dei dati in seguito a una variazione dei rischi derivante dalle operazioni di trattamento, ad esempio perché è entrata in uso una nuova tecnologia o perché i dati personali vengono utilizzati per una finalità diversa.

Le operazioni di trattamento o dei dati possono evolversi rapidamente e potrebbero emergere nuove vulnerabilità. Di conseguenza, va osservato che la revisione di una valutazione d'impatto sulla protezione dei dati non è utile soltanto ai fini di un miglioramento continuo, bensì anche fondamentale per mantenere il livello di protezione dei dati in un ambiente che muta nel corso del tempo. Una valutazione d'impatto sulla protezione dei dati potrebbe rendersi necessaria anche perché il contesto organizzativo o sociale per l'attività di trattamento è mutato, ad esempio perché gli effetti di determinate decisioni automatizzate sono diventati più significativi oppure perché nuove categorie di interessati sono diventati vulnerabili alla discriminazione.

La valutazione di impatto rappresenta quindi uno strumento necessario alla concretizzazione del principio della “privacy by design”, che impone al titolare, fin dalla fase di progettazione, di effettuare una valutazione del trattamento dei dati che intende avviare e delle misure ed accorgimenti da adottare per poter operare in termini di conformità rispetto alla normativa di riferimento. Infatti, l’art. 25 “protezione dei dati fin dalla progettazione e protezione per impostazione predefinita” del già citato Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 prevede che, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare del trattamento metta in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, ed a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del medesimo regolamento e tutelare i diritti degli interessati. Inoltre, lo stesso art. prevede che il titolare metta in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, sia rispetto alla quantità dei dati personali raccolti, alla portata del trattamento, al periodo di conservazione ed all'accessibilità e, in particolare, che per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Sotto il profilo metodologico, secondo il Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 e delle Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato” ai fini del Regolamento (UE) 2016/679 adottate il 04/04/2017 (ultima modifica del 04/10/2017), oltre che dell’abbondante

documentazione prodotta dall'Autorità Garante nazionale, sono Il titolare e il responsabile del trattamento – anche attraverso strutture tecniche a questo deputate – che provvedono a sviluppare la valutazione di impatto (il Garante indica la preferenza rispetto ad una "squadra" che possa portare avanti la valutazione, in modo che più componenti possano dare ognuno un diverso e qualificato contributo). Il DPO (Data Protection Officier/Responsabile Protezione dei Dati) deve analizzare, proporre eventuali migliorie ed approvare anche con i necessari profili di terzietà e le prerogative (in termini di autonomia e riconoscimento di funzione/posizione più volte dettati dalla stessa Autorità Garante) il rapporto per sovrintendere, successivamente, all'attuazione delle misure di sicurezza proposte.
Nel caso di specie, pur disponendo di un numero non particolarmente significativo in termini assoluti di sistemi di ripresa, l'apparato di videosorveglianza del Comune di Valfenera ha un'architettura impiantistica e gestionale che si presta al suo utilizzo per diversi scopi e funzionalità, tali da rendere necessario un intervento valutativo organico e generale che ha necessariamente richiesto un'analisi ricognitiva condotta direttamente dal DPO, a supporto del titolare e del responsabile del trattamento. Tale azione risulta coerente con i dettami della disciplina comunitaria e con le indicazioni dell'Autorità Garante in quanto garantisce un'analisi approfondita e critica dei sistemi esistenti e dei trattamenti che l'Amministrazione è intenzionata ad attivare. Inoltre, la posizione di terzietà del DPO è assicurata dalla sua indipendenza funzionale dalla struttura incaricata della progettazione ed esecuzione degli interventi tecnici e dal titolare.

Sono adottati come riferimento metodologico e per le pertinenti valutazioni i seguenti documenti:

- Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - Versione 2.0 adottate il 29/01/2020;
- Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679 adottate il 04/04/2017 (ultima modifica del 04/10/2017).

Inoltre, si è proceduto, come da indicazioni dell'Autorità Garante nazionale, ad una valutazione preliminare della DPIA attraverso il software messo a disposizione dalla CNIL (Autorità francese per la protezione dei dati) denominato PIA (Privacy Impact Assesment) che, pur non costituendo un modello a cui fare riferimento per ogni tipologia di trattamento, offre in ogni caso un focus semplificato sugli elementi principali di cui si compone la valutazione di impatto.

Ai fini del presente documento, e riguardo all'ambito principale di impiego del sistema di videosorveglianza del Comune di Valfenera, si intende:

- ai sensi del D.M. Interno del 05/08/2008, per "incolumità pubblica" l'integrità fisica della popolazione e per "sicurezza urbana" un bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità à nei centri urbani, la convivenza civile e la coesione sociale. (…) Il Sindaco interviene per prevenire e contrastare: a) le

situazioni urbane di degrado o di isolamento che favoriscono l'insorgere di fenomeni criminosi, quali lo spaccio di stupefacenti, lo sfruttamento della prostituzione, l'accattonaggio con impiego di minori e disabili e i fenomeni di violenza legati anche all'abuso di alcool; b) le situazioni in cui si verificano comportamenti quali il danneggiamento al patrimonio pubblico e privato o che ne impediscono la fruibilità e determinano lo scadimento della qualità urbana; c) l'incuria, il degrado e l'occupazione abusiva di immobili tali da favorire le situazioni indicate ai punti a) e b); d) le situazioni che costituiscono intralcio alla pubblica viabilità o che alterano il decoro urbano, in particolare quelle di abusivismo commerciale e di illecita occupazione di suolo pubblico; e) i comportamenti che, come la prostituzione su strada o l'accattonaggio molesto, possono offendere la pubblica decenza anche per le modalità con cui si manifestano, ovvero turbano gravemente il libero utilizzo degli spazi pubblici o la fruizione cui sono destinati o che rendono difficoltoso o pericoloso l'accesso ad essi;

- ai sensi della L. 18/04/2017, n. 48 (conversione in legge del D.L. 20/02/2017, n. 14 recante disposizioni urgenti in materia di sicurezza delle Città) per “sicurezza urbana” il bene pubblico che afferisce alla vivibilità ed 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 dei più elevati livelli di coesione sociale e di convivenza civile.

Sono escluse dalle finalità di “incolumità pubblica e sicurezza urbana” le attività di prevenzione o accertamento dei reati che possono invece essere disposti dall’Autorità Giudiziaria o disciplinati in specifici protocolli.

Ai fini del presente documento ed ai sensi del Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, si intendono inoltre per:

1) “dato personale”: qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) “trattamento”: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) “limitazione di trattamento”: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) “profilazione”: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) “pseudonimizzazione”: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) “archivio”: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) “titolare del trattamento”: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) “responsabile del trattamento”: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) ”destinatario”: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) “terzo”: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) “consenso dell'interessato”: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante

dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) “violazione dei dati personali”: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) “dati genetici”: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) “dati biometrici”: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

15) “dati relativi alla salute”: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) “autorità di controllo”: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51; 4.5.2016 L 119/34 Gazzetta ufficiale dell'Unione europea IT.

Inoltre, per quanto sovrapponibili nella loro *ratio* alla disciplina ad oggi applicabile (richiamo alla ormai abrogata L. 675/1996) si segnalano i pur risalenti Provvedimenti dell’Autorità Garante nazionale:

- Garante 21/10/1999, in Bollettino n. 10, pag. 80 [doc. web n. 42288]

La L. 675/1996 definisce "dato personale" qualunque informazione relativa a persone identificate o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione. Ne consegue che debbono essere considerati dati di carattere personale anche le registrazioni effettuate mediante l´uso di telecamere che, per l´ampiezza dell´angolo visuale, la qualità degli strumenti, o altre caratteristiche della ripresa, pur non rendendo direttamente identificabili in maniera chiara ed univoca le persone inquadrate, ne permettano l´identificazione attraverso il collegamento con altre fonti conoscitive, quali foto segnaletiche, identikit o archivi di polizia contenenti immagini.

- Garante 17 /02/2000, in Bollettino n. 11/12, pag. 73 [doc. web n. 40041]
- Garante 07/03/2000, in Bollettino n. 11/12, pag. 76 [doc. web n. 30987]

Le registrazioni effettuate mediante l´uso di telecamere non contengono sempre e necessariamente dati di carattere personale, in quanto la distanza, l´ampiezza dell´angolo visuale e la qualità degli strumenti possono non rendere identificabili le persone inquadrate; comunque, ciò non esclude l´applicazione della normativa sulla tutela della riservatezza, in quanto l´art. 1 della legge n. 675/1996 definisce "dato personale" qualunque informazione relativa a persone identificate o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione (ad esempio, attraverso il collegamento con altre fonti conoscitive quali foto segnaletiche, identikit o archivi di polizia contenenti immagini). Ai sensi dell´art. 27 della legge n. 675/1996, le finalità cui è preordinata l´installazione, da parte di un Comune, di impianti di videosorveglianza debbono rispondere alle funzioni istituzionali demandate all´ente dalla legge n. 142/1990, dal D.P.R. n. 616/1977, dalla legge n. 65/1986 (sull´ordinamento della Polizia Municipale), nonché dagli statuti e dai regolamenti comunali. In caso di realizzazione, da parte di un comune, di impianti di telecontrollo e videosorveglianza del territorio a fini di monitoraggio del traffico cittadino, per assicurare l´effettivo rispetto dei principi posti dall´art. 9 della legge n. 675/1996 è necessario procedere ad una precisa localizzazione delle telecamere e ad una limitazione delle modalità di ripresa delle immagini (memorizzazione, conservazione, angolo visuale delle telecamere e limitazione della possibilità di ingrandimento dell´immagine); inoltre, occorre un´attenta riflessione sul livello di dettaglio della ripresa dei tratti somatici e sulla necessità che siano evitate riprese di persone presso gli impianti volti unicamente a prevenire le violazioni del codice della strada.

- Garante 30/12/2002 [doc. web n. 1067284]

È lecito il trattamento dei dati effettuato dal Comune, in "contitolarità" con Questura e Comando dei Carabinieri, mediante l´installazione nel centro cittadino di un sistema di videosorveglianza, ove non emergano profili di illiceità del trattamento e risultino rispettati i limiti fissati dal Provvedimento di carattere generale emesso dal Garante in materia del 29/11/2000 (nel caso di specie il Garante ha rilevato che non erano state attivate alcune funzioni delle apparecchiature di ripresa particolarmente invasive quali i sistemi di registrazione delle conversazioni, di illuminazione ad infrarossi e di riconoscimento biometrico facciale).

- Garante 09/01/ 2003 [doc. web n. 1067775] e Garante 09/01/2003 [doc. web n. 1067813]

Non può essere accolto il ricorso con il quale l´interessato si oppone al trattamento delle immagini riprese dalle telecamere di un sistema di videosorveglianza istallato nel centro cittadino, ove, anche alla luce dei limiti fissati dal provvedimento di carattere generale emesso dal Garante in materia di videosorveglianza il 29/11/2000, non emergano profili di illiceità del trattamento, effettuato dal Comune in "contitolarità" con Questura e Comando dei Carabinieri.

1.2. ANALISI PRELIMINARE E CONTESTO

La valutazione di impatto, come anticipato, contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Le Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 adottate il 04/04/2017 (ultima modifica del 04/10/2017), tengono conto dei seguenti documenti:

- dichiarazione del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN WP 2186;
- linee guida sui responsabili della protezione dei dati del WP29 - 16/EN WP 2437;
- parere del WP29 sulla limitazione della finalità - 13/EN WP 2038;
- norme internazionali.

In linea con l'approccio basato sul rischio adottato dal G.D.P.R., secondo le Linee Guida non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento. Infatti, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando il trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche". Al fine di assicurare un'interpretazione coerente delle circostanze in cui è obbligatorio realizzare una valutazione d'impatto sulla protezione dei dati, le medesime Linee Guida mirano innanzitutto a chiarire tale nozione e a fornire criteri per gli elenchi che devono essere adottati dalle Autorità di protezione dei dati.

La funzione fondamentale dello scenario di rischio è di prevedere le conseguenze di un determinato evento, per poter su questa base definire le gli strumenti e le strategie di intervento con cui farvi fronte.

Le diverse forme di devianza e criminalità all'interno delle aree urbane destano nell'opinione pubblica un particolare allarmismo determinato in buona parte dalle continue rappresentazioni ed informazioni veicolate dagli organi di informazione ed amplificate, sotto certi aspetti, dai social network. Il trattare ripetutamente e quasi sistematicamente atti di violenza e comportamenti illeciti, che si fanno largo nelle coscienze e nell'immaginario comune, alimentano nei cittadini la paura di essere oggetto di violenza e favoriscono il diffondersi dell'insicurezza.
Premessa necessaria alla definizione dello scenario di rischio è la sintetica definizione di "criminalità e devianza" a cui ci si riferisce rispetto agli scopi della videosorveglianza su larga scala

associata alle “riprese intelligenti” (anche potenziali) che potrebbero caratterizzare il sistema comunale.
Se è pur vero che l’impiego delle telecamere assolve, per buona parte dei reati, una concreta funzione investigativa “a posteriori”, altrettanto vero è che espande anche potenzialmente la sua efficacia come deterrente rispetto a comportamenti illeciti o, in caso di adozione di sistemi cd. “intelligenti” (come nel caso di specie anche i sistemi di ripresa OCR “Optical Character Recognition” in grado di identificare le targhe dei veicoli in transito associata ad altri elementi caratteristici), anche come sistema di allarme che può garantire un intervento operativo immediato.

Per quanto di interesse per la redazione del presente documento, l’analisi della pericolosità del territorio, intesa come possibilità di accadimento di eventi o fatti significativi connessi alla necessità di attivare il sistema di videosorveglianza del Comune di Valfenera, deve avere come riferimento principale la vulnerabilità del sistema antropico intesa nell’accezione riconducibile alla “incolumità pubblica” ed alla “sicurezza urbana” (oltre che al più complesso concetto di “sicurezza civile”.
In sintesi, lo scenario di rischio su cui si innesta la videosorveglianza (in termini astratti) come strumento per affrontarlo e mitigarlo può essere così costruito:

	Offesa attiva (intenzionale)	Offesa passiva (non intenzionale)
Fenomeno fisico	• Vandalismo (arredo urbano danneggiato, veicoli, strutture pubbliche/private violate e danneggiate) • Edifici occupati	• Edifici abbandonati • Aree pubbliche soggette ad incuria • Relazioni conflittuali tra generazioni, tra residenti, tra comunità
Fenomeno sociale	• Consumo di sostanze stupefacenti • Prostituzione • Mendicanza • Vendita abusiva di beni • Somministrazione illecita di alcolici • Molestie e schiamazzi	

Il fenomeno fisico passivo trasmette al cittadino un senso di incuria e di disinteresse pubblico e privato, mentre quello attivo (fenomeno sociale attivo e l’inciviltà sociale, legati ad una volontà di violazione della norma, morale, sociale e legale da parte di un attore) determina un senso di sfiducia nei meccanismi di controllo sociale, sia pubblici che privati.

È ancora possibile identificare delle minacce alla sicurezza (sicurezza percepita) discriminando, tra le situazioni presenti in aurea urbana e frazionale, tra "inciviltà" e reati:

Situazioni potenzialmente presenti

"inciviltà"	reati
▪ Sporcizia e rifiuti pericolosi (deiezioni, rifiuti ingombranti, scarti di lavorazione, vernici e solventi, siringhe	▪ Borseggio e scippo
▪ Situazioni specifiche (campi nomadi cittadini)	▪ Spaccio di sostanze stupefacenti
▪ Presenza diffusa di soggetti molesti ed indesiderati	▪ Vandalismo e danneggiamento
▪ Aree verdi abbandonate	▪ Furto (in abitazione ed altro)
▪ Edifici pubblici in stato di abbandono	▪ Risse
▪ Scarsa illuminazione pubblica	▪ Truffe domestiche
▪ Gruppi di persone rumorose	▪ Occupazione abusiva di edifici
▪ Presenza di prostituzione	▪ Situazioni specifiche

Il grado di minaccia percepito dai cittadini rispetto a possibili situazioni di "inciviltà" è in prevalenza legato alla "qualità dei luoghi" (pulizia, aree verdi, illuminazione) con l'eccezione connessa alla presenza di soggetti molesti ed indesiderati. Tale indicazione generale trova specifica conferma nell'ambito dei reati, laddove la minaccia è legata non solo alla microcriminalità che attenta alle proprietà, sia in termini di appropriazione (furti, scippi, borseggi) sia in termini di danneggiamento (le diverse forme di vandalismo su beni pubblici e privati, individuali e collettivi, che sono pur sempre una parte dello spazio urbano) ma anche al radicamento di una diffusa "criminalità di strada".

Lo scenario complessivo si basa quindi su una concorrenza potenziale di elementi di valutazione che derivano sia dal vissuto individuale, sia dalle informazioni presenti nelle reti di relazione che dall'esposizione ai mezzi di comunicazione

Rispetto ai rischi che potenzialmente possono gravare sugli interessati per effetto del trattamento dei dati personali attraverso il sistema di videosorveglianza del Comune di Valfenera, il bene da tutelare è la libertà dei cittadini, che devono poter circolare nei luoghi pubblici senza dover subire ingerenze eccessive o improprie nella loro riservatezza. **Tale libertà va, quindi, opportunamente contemperata con le esigenze di sicurezza che si intende garantire agli stessi cittadini.**
Nell'installazione e gestione del sistema di videosorveglianza, come evidenziato dall'Autorità Garante nazionale già con il Provvedimento generale del 08/04/2010, occorre fissare dei requisiti ì stringenti per evitare che l'attività di videosorveglianza si espanda fino a limitare i diritti del

cittadini. Con esso il Garante ha determinato il bilanciamento tra i diritti dei cittadini e la sicurezza e la prevenzione dei reati stabilendo che l'attività di videosorveglianza è consentita se sono rispettati i seguenti principi: liceità, necessità, proporzionalità e finalità.

Considerate le ridotte dimensioni territoriali e demografiche del Comune di Valfenera, lo scenario di rischio riconducibile alla "necessarietà" ed utilità della videosorveglianza quale valido strumento di mitigazione deve essere ricondotto a scenari di minore ampiezza e gravità rispetto al modello generale sotteso al vigente impianto normativo. In particolare lo scenario locale afferisce e fenomeni di estemporaneo danneggiamento di immobili/strutture pubbliche per uso improprio o atti vandalici registrati nel recenti passato, oltre ad una generale esigenza di monitoraggio del traffico in entrate/uscita dal centro abitato anche in ossequio alle esigenze investigative manifestate in modo ricorrente dalla Forze di Polizia,

La videosorveglianza è lecita se è funzionale allo svolgimento delle funzioni istituzionali (nel caso di Enti Pubblici), oppure se vi è un consenso libero ed espresso da parte delle persone riprese dalle telecamere.

Il requisito della necessità limita l'uso di sistemi di videosorveglianza ai soli casi nei quali l'obiettivo non può essere raggiunto con modalità diverse, ad esempio utilizzando inquadrature anonime o predisponendo l'impianto in modo che mantenga le riprese solo per il periodo di tempo necessario, con ciò evitando usi eccessivi o sproporzionati. Inoltre deve essere rispettato il principio di minimizzazione dei dati, con riferimento alle scelte delle modalità di ripresa e dislocazione delle telecamere, nonché alla gestione delle varie fasi del trattamento. I dati trattati devono comunque essere pertinenti e non eccedenti rispetto alle finalità perseguite.

Il requisito di proporzionalità obbliga a ricorrere ai sistemi di videosorveglianza solo come misura ultima di controllo, cioè quando altre misure si siano rivelate insufficienti oppure inattuabili. Non è ammissibile, quindi, l'uso di telecamere solo perché l'impianto è meno costoso rispetto ad altre forme di controllo.

Il principio di finalità stabilisce che chi installa le telecamere può perseguire solo fini di sua pertinenza, cioè può utilizzare le telecamere solo per il controllo della sua attività, ma non può mai utilizzare le telecamere per finalità esclusivamente di sicurezza pubblica, che sono, invece, di competenza delle autorità giudiziarie ed amministrative.

2. ARCHITETTURA DI RETE ED APPARATI

Secondo le Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - Versione 2.0 adottate il 29/01/2020, in termini generali un sistema di videosorveglianza (denominato VSS) è costituito da dispositivi analogici e digitali nonché da software per acquisire immagini, gestirle e mostrarle a un operatore. I suoi componenti sono categorizzabili come segue:

- ambiente video: acquisizione immagini, interconnessioni e gestione immagini: o l'acquisizione delle immagini serve a generare un'immagine del mondo reale in un formato tale da poter essere utilizzata dal resto del sistema, o le interconnessioni comprendono tutte le trasmissioni di dati all'interno dell'ambiente video, vale a dire connessioni e comunicazioni (cavi, reti digitali e trasmissioni wireless). Le comunicazioni descrivono tutti i segnali video e dati di controllo, che potrebbero essere digitali o analogici, o la gestione delle immagini comprende l'analisi, la conservazione e la presentazione di un'immagine o di una sequenza di immagini;

- gestione del sistema e funzioni logiche: gestione dei dati e delle attività, comprendente la gestione dei comandi degli operatori e delle attività generate dal sistema (procedure di allarme, operatori di allarme), o le interfacce con altri sistemi potrebbero includere la connessione ad altri sistemi di sicurezza (controllo accessi, allarme antincendio) o non legati alla sicurezza (sistemi di gestione edifici, riconoscimento automatico delle targhe);

- sicurezza: riservatezza, integrità e disponibilità del sistema e dei dati, comprensiva della sicurezza fisica di tutti i componenti del sistema e il controllo dell'accesso al sistema, oltre alla prevenzione della perdita o della manipolazione dei dati.

Coma da progetto esaminato, a cui si rimanda per glia spetti tecnici di dettaglio, il sistema di videosorveglianza del Comune di Valfenera è costituito da una rete semplice di impianti riconducibili due ambiti d'intervento e due differenti tipologie di sistemi di ripresa che andranno a costituire, una volta a regime e tenendo conto dei possibili futuri sviluppi dell'impianto, una diffusa infrastruttura di supporto al controllo delle aree sensibili comunali:
- una prima tipologia riguarda interventi di tipo generico, attraverso telecamere "di contesto" che permettono il controllo di aree pubbliche riconducibili a luoghi sensibili o a particolari zone oggetto d'interesse;
- una seconda tipologia d'intervento è volta al controllo degli accessi veicolari sulle principali direttrici stradali, attraverso telecamere per lettura targhe (OCR Optical Character Recognition)

2.1. SPECIFICHE FUNZIONALI

Il sistema adottato dal Comune di Valfenera, con riferimento alla documentazione visionata, risalente all'anno 2019 è riconducibile al progetto denominato "messa in sicurezza dell'area urbana mediante l'ampliamento dei sistema di videosorveglianza" (progetto esecutivo) contempla la fornitura di telecamere ad alta risoluzione per finalità di monitoraggio delle aree soggette a rischio di eventi criminosi oltre che per il controllo, tramite sistemi ANPR e lettura targhe, dei varchi in ingresso del territorio comunale.

Il progetto, relativo ai sistemi di ripresa già esistenti ed esaminati nell'ambito della presente valutazione di impatto, si è posto l'obiettivo di mettere in sicurezza le zone del territorio comunale definite "sensibili"agli atti criminosi e che "mira a dare ai soggetti competenti (Polizia Municipale, Forze dell'Ordine, Vigilanza privata ..) tutti gli strumenti necessari per poter intervenire non solo post-evento ma anche, eventualmente, in tempo reale durante l'accadimento del fatto".

Il sistema previsto a progetto utilizza di tecnologia WIFI per collegare tutti i sistemi di ripresa la cui architettura di rete consente di veicolare i dati ad un "centro stella" ubicato presso il palazzo comunale. Il server di registrazione è collocato presso il Comune di Ferrere, a sua volta connesso con il Comune di Valfenera con rete intranet.

inoltre, il medesimo sistema garantisce la compatibilità tecnologica con gli apparati in uso ai Comuni limitrofi e la loro eventuale interconnessione oltre che l'eventuale collegamento con le sale operative delle l'interconnessione con le Forze dell'Ordine, otre che interagire con le principali banche dati rilevanti per lo scopo (M.T.C.T. e Sistema Centralizzato Nazionale Transiti S.C.N.T.T.).

Il sistema previsto permette la conservazione a sistema dei dati targa e delle immagini di contesto acquisite (flusso video) e si interfaccia con le principali marche di telecamera per lettura targhe (OCR Optical Character Recognition), elemento ritenuto dal progettista fondamentale per non vincolare tecnicamente e/o commercialmente l'Amministrazione per l'espansione futura del sistema. Il database accoglierà tutti i dati targa in ingresso senza limitazioni di memoria grazie allo storage correttamente dimensionato e protetto da backup RAID jbod. Il software previsto non ha limiti come numero di client pc a cui rispondere ed è strutturato come una piattaforma aperta installata su un server a cui più client possono accedervi con specifiche credenziali. Ogni credenziale può essere nominativa, anche active directory compliance ed essere autorizzata come "operatore abilitato" a tutte o parte delle funzioni del sistema, oppure consultabile direttamente dal server.

<u>Funzioni principali del software di lettura targhe</u>

Le apparecchiature individuate a progetto e successivamente installate prevedono l'integrazione specifica comunemente definita ANPR, in grado di interfacciarsi con sistemi di ripresa che garantiscono un flusso video RSTP in grado di analizzare il flusso video e per ricavarne una targa, in particolare con le funzioni di Lettura Targhe Italiane e Estere, Gestione Black List, Interfacciamento con Database Ministeriali per controllo RCA, Revisione, Interfacciamento con Database stranieri per Controllo RCA, e con le seguenti funzionalità operative:

- Interfaccia Web per la gestione dei transiti/ricerche/report/statistiche
- Possibilità importazione DB SIVES, Allarmi Mail personalizzabili
- Possibilità di interfacciamento con modulo ministeriale SCNTT.
- Accesso remoto all'interfaccia Web per terze parti
- Esportazione delle liste e possibilità di collegamento via Web per visualizzazioni allarmi real-time su tablet/smartphone/telefono con qualsiasi sistema operativo.

Inoltre i sistema previsto, tramite apposito modulo, sarà in grado di verificare la copertura assicurativa, la data dell'ultima revisione e se il veicolo risulta rubato e in caso di un veicolo non in regola, comporterà un allarme finalizzato alla successiva azione di fermo del veicolo.
E'inoltre prevista la dotazione dell'App Mobile per la visualizzazione del traffico veicolare che consente l'acquisizione delle seguenti informazioni:

- classificazione dei veicoli in transito;
- individuazione targhe con mancato pagamento assicurazione;
- individuazione veicoli non in regola con la revisione;
- nazionalità della targa rilevata;

Sfruttando il Client in centrale operativa è possibile disporre di molteplici informazioni sulla base della tipologia di sistema di ripresa installato e potenzialmente incrementabile a:

- statistiche relative al tracciamento del flusso veicolare, velocità di percorrenza, allert congestionamento traffico, superamento valori inquinamento dell'aria (pm10 e pm2.5 solo con l'acquisto di sensori opzionali), ingresso in città di veicoli pericolosi (codici kemler):
- statistiche sulla tipologia di veicoli in ingresso (auto, motocicli, furgoni, autocarri, …)
- statistiche sulla classe ambientale dei veicoli in ingresso e/o uscita per richieste visure in motorizzazione con l'accuratezza del dato pari al 95%
- marca e modello dei veicoli
- colore dei veicoli
- tipologia dei veicoli
- gestione del database targhe: consultazione, ricerche e statistiche avanzate
- gestione del database immagini di contesto: visualizzazione del live, del registrato e relativo download e aree di interesse

Rispetto alla qualità e tipologia delle apparecchiature previste per la prima implementazione del sistema (anno 2019) si rimanda alla relazione tecnica riconducibile al progetto licenziato dal Comune di Valfenra, agli atti dell'Amministrazione.

Nel dicembre 2021, il Comune di Valfenera ha licenziato un nuovo progetto denominato “realizzazione di opere per la messa in sicurezza dell’area urbana mediante l’ampliamento dell’impianto di videosorveglianza” che prevede la fornitura di telecamere di contesto e lettura targhe per finalità di monitoraggio delle aree a rischio del territorio comunale.

Rispetto alla qualità e tipologia delle apparecchiature previste per la seconda implementazione del sistema (anno 2021) si rimanda alla relazione tecnica riconducibile al progetto licenziato dal Comune di Valfenera, agli atti dell’Amministrazione.

3. VALUTAZIONE DI IMPATTO

Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenti rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, può essere ammesso solo nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti dall’Autorità Garante per la protezione dei dati personali nell'ambito di una verifica preliminare all'inizio del trattamento.

Analogamente, già il pur risalente Provvedimento dell’Autorità Garante per la protezione dei dati personali in materia di videosorveglianza del 08/04/2010 (G.U. n. 99 del 29/04/2010) precisava che i trattamenti di dati personali nell'ambito di una attività di videosorveglianza devono essere effettuati rispettando le misure e gli accorgimenti prescritti come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello del titolare quando vi sono rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare.

Le Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video e l’Autorità Garante per la protezione dei dati personali ricomprende nelle ipotesi da sottoporre a valutazione di impatto anche i sistemi di raccolta delle immagini associate a dati biometrici, vale a dire i sistemi di videosorveglianza dotati di software che permetta il riconoscimento della persona tramite collegamento o incrocio o confronto delle immagini rilevate (morfologia del volto) con altri specifici dati personali, in particolare con dati biometrici, o sulla base del confronto della relativa immagine con una campionatura di soggetti precostituita alla rilevazione medesima.

Una smile necessità di valutazione sussiste con riferimento a sistemi c.d. “intelligenti”, che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli. Tali sistemi devono considerarsi eccedenti rispetto alla normale attività di videosorveglianza, in quanto possono determinare effetti particolarmente invasivi sulla sfera di autodeterminazione dell'interessato e, conseguentemente, sul suo comportamento. Il relativo utilizzo risulta comunque giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati, da verificare

caso per caso sul piano della conformità ai principi di necessità, proporzionalità, finalità e correttezza.

Occorre anche valutare approfonditamente l'utilizzo di sistemi integrati di videosorveglianza nei casi in renda necessario l'allungamento dei tempi di conservazione dei dati delle immagini registrate oltre il previsto termine massimo di 7 giorni derivante da speciali esigenze di ulteriore conservazione, a meno che non derivi da una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria in relazione a un'attività investigativa in corso.

Il sistema di videosorveglianza che sotto il profilo della piattaforma gestione e trattamento dei dati deve essere considerato unitario, può potenzialmente essere ricondotto ai sistemi c.d. “intelligenti” come identificati e descritti dal Provvedimento dell’Autorità Garante per la protezione dei dati personali in materia di videosorveglianza del 08/04/2010 (G.U. n. 99 del 29/04/2010 e contemplate dalle Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, che trovano dimora nel Regolamento Generale Sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 all’art. 35, paragrafo 3, lettera c), che impone l’esecuzione di una valutazione d’impatto sulla protezione dei dati in caso di sorveglianza sistematica su vasta scala di un’area accessibile al pubblico, e all’articolo 37, paragrafo 1, lettera b), che impone ai responsabili del trattamento di designare un responsabile della protezione dei dati se la tipologia di trattamento, per sua natura, richiede il monitoraggio regolare e sistematico degli interessati.

Nel suo complesso, quindi il sistema di videosorveglianza del Comune di Valfenera integra la fattispecie di cui all’art. 35 “Valutazione d'impatto sulla protezione dei dati” Regolamento Generale Sulla Protezione Dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 e, in particolare configura un trattamento di dati personali riconducibile alla “sorveglianza sistematica su larga scala di una zona accessibile al pubblico” e necessità della predisposizione di una valutazione di impatto preveniva.

La valutazione di impatto, secondo quanto previsto dalla citata disciplina comunitaria, contiene:

3.1 DESCRIZIONE SISTEMATICA DEI TRATTAMENTI PREVISTI

In via preliminare, non può dubitarsi che anche l'immagine di una persona, quando in qualche modo venga visualizzata o impressa, possa costituire "dato personale" ai sensi dell’art. 4, punto 1) del Regolamento Generale Sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016: “qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”) in quanto permette di identificare o rendere identificabile una persona fisica, anche in caso di “non registrazione” delle immagini,

poiché anche la mera visualizzazione delle stesse, comporta la raccolta e quindi il trattamento di dati personali[1].

Di conseguenza, l'acquisizione di immagini provenienti dall'ambito/contesto urbano ed extraurbano attraverso il sistema videosorveglianza del Comune di Valfenera integra la fattispecie di "trattamento dei dati personali" di cui al Regolamento Generale Sulla Protezione Dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 ("trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, … …)

Il trattamento dei dati personali (immagini) consiste sostanzialmente nell'acquisizione e conservazione del flusso video provenienti dalle telecamere installate in area urbana e nel territorio frazionale.

La rilevazione delle immagini riconducibili al trattamento assoggettabile a valutazione di impatto avviene potenzialmente grazie a telecamere di contesto e telecamere per lettura targhe (OCR Optical Character Recognition) che confluiscono presso una "centrale operativa" dislocata presso il palazzo comunale (piattaforma di gestione e visualizzazione immagini sia in diretta/sincronia che in modalità differita) con limitazione all'accesso.

Per le telecamere ad ottica fissa viene registrato/acquisito un flusso di ripresa "non elaborata" e attualmente privo dell'algoritmo di analisi.

È possibile, tuttavia, potenzialmente abilitare le telecamere ad ottica fissa, a cui asservire uno specifico software, ad effettuare operazioni di cd. "videoanalisi".

La "videoanalisi" (o, in termini più precisi VCA Video Context Analysis), nelle varie declinazioni ormai possibili costituisce un insieme di tecniche di computer vision che consentono l'analisi e l'interpretazione critica di un flusso video allo scopo di comprenderne il contenuto e di "annotarlo" automaticamente sottoforma di "metadati" che, se appositamente configurati, possono produrre "allarmi" per segnalare eventi all'operatore o per registrare il verificarsi di determinate condizioni nella contesto inquadrato dalla telecamera

Il sistema di videosorveglianza del Comune di Valfenera, se adeguatamente implementato, può potenzialmente garantire diverse funzionalità che potranno essere attivate in base alle specifiche esigenze operative dell'Amministrazione, oltre che messe a disposizione della Questura e del Comando Provinciale dei Carabinieri per i compiti istituzionali e nei limiti e con le prerogative del caso. La Valutazione di Impatto considera anche questa condizione potenziale, in modo da garantire migliore libertà operativa all'Amministrazione in caso di future implementazioni della capacità del sistema.

[1] Cass. Pen. Sez. 2 27/04/2015, n. 17440 e Cass. Civ. Sez. 1 24/04/2012, n. 14346/2012

Per quanto di interesse rispetto alla Valutazione di Impatto, occorre sottolineare che il progettista ha previsto per i sistemi che saranno attivati, l'implementazione con specifici trigger che reagiscono a eventi esterni quali il movimento o la presenza intrusi all'interno di contorni definiti in fase di programmazione, oltre attraversamento di una linea definita,

Di conseguenza, le funzionalità potenzialmente attivabili a seguito di consentito sviluppo dell'impianto e riconducibili alla video context analysis sono di norma basate sull'algoritmo di blob motion tracking che "lavora" sulla separazione del background (sfondo statico delle immagini) dal foreground (immagini in movimento sopra il background) permettendo di individuare ed "isolare" gli elementi in movimento (blob) in modo relativamente affidabile e, di conseguenza, in funzione dei parametri di configurazione assegnati al sistema. In assenza di tali specifiche funzionalità si rimanda necessariamente la valutazione circa l'incidenza dell'impiego delle differenti possibilità di "video analisi" sul trattamento, che potrà essere effettuata disponendo delle caratteristiche tecniche dei prodotti eventualmente acquisiti (licenze).

La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso del sistema videosorveglianza del Comune di Valfenera deve essere limitata ai 7 giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione o eventuali disposizioni dell'Autorità Giudiziaria per specifiche esigenze investigative o per quanto necessario per ricostruire l'evento, per le finalità previste dall'apposito Regolamento. Oltre il tempo previsto dall'art. 6 della L. 38/2009, le immagini sono cancellate mediante registrazione in sovrascrittura. Le immagini sono custodite in maniera protetta, limitatamente alla tecnologia in uso, in server dedicati e su reti informatiche non liberamente accessibili.

Il trattamento, in senso lato, può essere considerato anche come esteso alla "modalità di funzionamento" della piattaforma di visualizzazione/gestione del flusso video. Questa precisazione, ai fini del presente documento si rende necessaria in quanto le modalità di visualizzazione delle immagini in sincronia consentono al singolo operatore l'apprezzamento di particolari ritenuti potenzialmente significativi, anche considerato il contesto territoriale in cui si sviluppa il trattamento dei dati.

Pertanto, il trattamento che si intende effettuare mediante l'uso del sistema videosorveglianza del Comune di Valfenera è così sintetizzabile:

- acquisizione immagini (creazione flusso video)
- registrazione del flusso video su piattaforma di registrazione (con residenza presso il server di registrazione Comune di Ferrere)
- potenziale video analisi (lettura targhe OCR Optical Character Recognition)
- potenziale registrazione del flusso video sottoposto a video analisi su piattaforma di registrazione o conservazione dei dati (lista transiti, black list nel caso dei sistemi di lettura targhe OCR Optical Character Recognition)
- visualizzazione del flusso video sia in modalità sincrona che in tempo differito, sia in modalità "neutra" che potenzialmente in modalità "video analisi" (con allarmi)

- visualizzazione immagini presa in carico della telecamera da parte di un operatore,

3.2. FINALITÀ DEL TRATTAMENTO, COMPRESO L'INTERESSE LEGITTIMO PERSEGUITO DAL TITOLARE DEL TRATTAMENTO

L'art. 5 "Principi applicabili al trattamento di dati personali" del Regolamento Generale Sulla Protezione Dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 prevede che i dati personali siano:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (liceità, correttezza e trasparenza);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
d) esatti e, se necessario, aggiornati e, se necessario, tempestivamente cancellati o rettificati;
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (integrità e riservatezza).

Il sistema videosorveglianza del Comune di Valfenera comporta il trattamento di dati personali che, in relazione ai luoghi di installazione delle telecamere, interessano i soggetti ed i mezzi di trasporto che transitano nell'area interessata. Il Comune Valfenera promuove ed attua, per la parte di competenza e nei limiti delle risorse concretamente disponibili, politiche di controllo del territorio, integrate con organi istituzionalmente preposti alla sicurezza pubblica. A tal fine l'Amministrazione locale, autonomamente o su richiesta delle autorità di pubblica sicurezza e degli organi di polizia, può disporre l'utilizzo degli impianti comunali di videosorveglianza ai fini di prevenzione e repressione di atti delittuosi.

Il sistema videosorveglianza del Comune di Valfenera può essere impiegato in via prioritaria:

a) con lo scopo di prevenire e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale secondo quanto previsto dal D.M. Interno del 05/08/2008 e dalla L. 18/04/2017, n. 48 (conversione in legge del D.L 20/02/2017, n. 14 recante disposizioni urgenti in materia di sicurezza delle Città) che definiscono e circoscrivono gli ambiti di applicazione della "incolumità pubblica e della sicurezza urbana" ed i conseguenti interventi del Sindaco;

b) acquisire prove nell'ambito dei procedimenti che dipendono dalla competente Autorità Giudiziaria, secondo le norme del Codice di Procedura Penale;
c) tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale, compresi gli edifici scolastici;
d) consentire, su espressa richiesta delle parti interessate ed aventi titolo, di fornire informazioni relative a sinistri stradali.

e potenzialmente per:

e) monitorare il traffico (identificare in tempo reale, se necessario, punti della rete viaria cittadina soggetto a rallentamenti o incidenti per consentire le necessarie procedure di allarme, rilevazione di dati anonimi per l'analisi dei flussi di traffico utili anche per la predisposizione di eventuali interventi alla viabilità)
f) rilevare violazioni al Codice della Strada;
g) tutelare le varie matrici ambientali e, in particolare, accertare i fenomeni di abbandono rifiuti e le violazioni alle disposizioni relative all'igiene urbana ed alle modalità di conferimento dei rifiuti urbani ed assimilabili;
h) supportare le attività di previsione e prevenzione di Protezione Civile e gli interventi operativi di emergenza, anche attraverso la rilevazione di dati anonimi per l'analisi dei flussi di traffico per la corretta definizione degli scenari di rischio legati alle vie di comunicazione ed al trasporto di merci pericolose, per la definizione del numero di soggetti presenti in aree pubbliche destinate ad venti di rilevanza locale, o per il controllo dell'accesso ad aree interdette o pericolose in caso di eventi calamitosi.

Le finalità sistema videosorveglianza del Comune di Valfenera sono conformi alle funzioni istituzionali demandate all'Amministrazione comunale in ossequio alle disposizioni dettate dal Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 ed al principio di liceità. Infatti il trattamento dei dati personali da parte del Comune di Valfenra rispetto alla videosorveglianza su area pubblica avviene (ed avverrà per quanto di prevista ulteriore attivazione) soltanto entro i limiti di competenza stabiliti in particolare dal D.Lgs 267/2000 e ss.mm.ii., dal D.P.R. 616/1977 e ss.mm.ii., dal D.Lgs. 112/1998, dalla L. 65/1986 e ss.mm.ii. sull'ordinamento della Polizia Municipale, dalla L.R. Piemonte 58/1987 e dalla L.R. Piemonte 57/1991, dal D.L. 92/2008 recante "Misure urgenti in materia di sicurezza pubblica" convertito con modificazioni in L. 125/2008, dalla L. 38/2009 dal D.M. Interno del 05/08/2008, dalla L. 48/2017 (conversione in legge del D.L. 20/02/2017, n. 14 recante disposizioni urgenti in materia di sicurezza delle Città).

Procedendo in maniera analitica:

- D.Lgs 267/20000 e ss.mm.ii., "Testo Unico delle Leggi sull'ordinamento degli Enti Locali" (cosi come modificato dal D.L. 20/02/2017, n. 14 "Disposizioni urgenti in materia di sicurezza delle Città" (poi convertito in L. 18/04/2017, n. 48) e dalla L. 24/07/2008, n. 125

“Conversione in legge, con modificazioni, del D.L. 23/05/2008, n. 92, recante misure urgenti in materia di sicurezza pubblica”

Art. 50 - Competenze del sindaco e del Presidente della Provincia

1. Il Sindaco e il Presidente della Provincia sono gli organi responsabili dell'amministrazione del Comune e della Provincia. 2. Il Sindaco e il Presidente della Provincia rappresentano l'Ente, convocano e presiedono la Giunta, nonché il Consiglio quando non e' previsto il Presidente del Consiglio, e sovrintendono al funzionamento dei servizi e degli uffici e all'esecuzione degli atti. 3. (…) essi esercitano le funzioni loro attribuite dalle Leggi, dallo Statuto e dai Regolamenti e sovrintendono altresì all'espletamento delle funzioni statali e regionali attribuite o delegate al comune e alla provincia. 4. Il Sindaco esercita altresì le altre funzioni attribuitegli quale autorità locale nelle materie previste da specifiche disposizioni di legge. 5. In particolare, in caso di emergenze sanitarie o di igiene pubblica a carattere esclusivamente locale le ordinanze contingibili e urgenti sono adottate dal Sindaco, quale rappresentante della comunità locale. Le medesime ordinanze sono adottate dal sindaco, quale rappresentante della comunità locale, in relazione all'urgente necessità di interventi volti a superare situazioni di grave incuria o degrado del territorio, dell'ambiente e del patrimonio culturale o di pregiudizio del decoro e della vivibilità urbana, con particolare riferimento alle esigenze di tutela della tranquillità e del riposo dei residenti, anche intervenendo in materia di orari di vendita, anche per asporto, e di somministrazione di bevande alcoliche e superalcoliche.) (…)

l’art. 54 “Attribuzioni del sindaco nelle funzioni di competenza statale”

1. Il Sindaco, quale ufficiale del Governo, sovrintende: a) all'emanazione degli atti che gli sono attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica; b) allo svolgimento delle funzioni affidategli dalla legge in materia di pubblica sicurezza e di polizia giudiziaria; c) alla vigilanza su tutto quanto possa interessare la sicurezza e l'ordine pubblico, informandone preventivamente il Prefetto. 2. Il Sindaco, nell'esercizio delle funzioni di cui al comma 1, concorre ad assicurare anche la cooperazione della polizia locale con le Forze di polizia statali, nell'ambito delle direttive di coordinamento impartite dal Ministro dell'interno – Autorità nazionale di pubblica sicurezza. (…) 4. Il Sindaco, quale ufficiale del Governo, adotta con atto motivato provvedimenti, anche contingibili e urgenti nel rispetto dei principi generali dell'ordinamento, al fine di prevenire e di eliminare gravi pericoli che minacciano l'incolumità pubblica e la sicurezza urbana. I provvedimenti di cui al presente comma sono preventivamente comunicati al prefetto anche ai fini della predisposizione degli strumenti ritenuti necessari alla loro attuazione. 4-bis. I provvedimenti adottati ai sensi del comma 4 concernenti l'incolumità pubblica sono diretti a tutelare l'integrità fisica della popolazione, quelli concernenti la sicurezza urbana sono diretti a prevenire e contrastare l'insorgere di fenomeni criminosi o di illegalità, quali lo spaccio di stupefacenti, lo sfruttamento della prostituzione, la tratta di persone, l'accattonaggio con impiego di minori e disabili, ovvero riguardano fenomeni di abusivismo, quale l'illecita occupazione di spazi pubblici, o di violenza, anche legati all'abuso di alcool o all'uso di sostanze stupefacenti.)) 5. Qualora i provvedimenti dai sindaci ai sensi dei commi 1 e 4 comportino conseguenze sull'ordinata convivenza delle popolazioni dei comuni contigui o limitrofi, il Prefetto

indice un'apposita conferenza alla quale prendono parte i sindaci interessati, il presidente della provincia e, qualora ritenuto opportuno, soggetti pubblici e privati dell'ambito territoriale interessato dall'intervento. (…)

- Statuto del Comune di Valfenera

Riprende sostanzialmente i contenuti e le disposizioni del D.Lgs 267/2000 e ss.mm.ii.

- D.P.R. 616/1977 "Attuazione della delega di cui all'art. 1 della L. 22/07/1975, n. 382

Art. 18. Polizia locale urbana e rurale

Le funzioni amministrative relative alla materia "polizia locale urbana e rurale" concernono le attività di polizia che si svolgono esclusivamente nell'ambito del territorio comunale e che non siano proprie delle competenti autorità statali.

Per quanto di interesse ed in relazione all'attribuzione ai Comuni delle funzioni di cui al Testo Unico delle Leggi di Pubblica Sicurezza (allora vigente) e ss.mm.ii. approvato con R.D. 18/06/1931, n. 773, e ss.mm.ii.;

Art. 19. Polizia amministrativa

(…) In relazione alle funzioni attribuite ai comuni il Ministero dell'interno, per esigenze di pubblica sicurezza, può impartire, per il tramite del commissario del Governo, direttive ai Sindaci che sono tenuti ad osservarle.

- D.Lgs 31/03/1998 n. 112 **"**Conferimento di funzioni e compiti amministrativi dello Stato alle regioni ed agli Enti Locali, in attuazione del Capo I della Legge 15/03/1997, n. 59**"**

Art. 108 Funzioni conferite alle regioni e agli Enti Locali

1. Tutte le funzioni amministrative non espressamente indicate nelle disposizioni dell'articolo 107 sono conferite alle regioni e agli enti locali e tra queste, in particolare: (…) c) sono attribuite ai comuni le funzioni relative: 1) all'attuazione, in ambito comunale, delle attività di previsione e degli interventi di prevenzione dei rischi, stabilite dai programmi e piani regionali; 2) all'adozione di tutti i provvedimenti, compresi quelli relativi alla preparazione all'emergenza, necessari ad assicurare i primi soccorsi in caso di eventi calamitosi in ambito comunale; 3) alla predisposizione dei piani comunali e/o intercomunali di emergenza, anche nelle forme associative e di cooperazione previste dalla legge 8 giugno 1990, n. 142, e, in ambito montano, tramite le Comunità Montane, e alla cura della loro attuazione, sulla base degli indirizzi regionali; 4) all'attivazione dei primi soccorsi alla popolazione e degli interventi urgenti necessari a fronteggiare l'emergenza; (…)

- L. 24/07/2008, n. 125 **"**Conversione in legge, con modificazioni, del D.L. 23/05/2008, n. 92, recante misure urgenti in materia di sicurezza pubblica"

Art. 6 (D.L 23/05/2008, n. 92 Modifica del testo unico di cui al D.L.gs 18/08/2000, n. 267, in materia di attribuzioni del Sindaco nelle funzioni di competenza statale) 1. L'articolo 54 del Testo Unico delle Leggi sull'ordinamento degli Enti Locali, di cui al D.Lgs 18/08/2000, n. 267, è sostituito dal seguente: "Art. 54 (Attribuzioni del Sindaco nelle funzioni di competenza statale). - 1. Il Sindaco, quale ufficiale del Governo, sovrintende: a) all'emanazione degli atti che gli sono attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica; b) allo svolgimento delle funzioni affidategli dalla legge in materia di pubblica sicurezza e di polizia giudiziaria; c) alla vigilanza su tutto quanto possa interessare la sicurezza e l'ordine pubblico, informandone preventivamente il Prefetto. 2. Il Sindaco, nell'esercizio delle funzioni di cui al comma 1, concorre ad assicurare anche la cooperazione della polizia locale con le Forze di polizia statali, nell'ambito delle direttive di coordinamento impartite dal Ministro dell'interno - Autorità nazionale di pubblica sicurezza. 4. Il Sindaco, quale ufficiale del Governo, adotta con atto motivato provvedimenti, anche contingibili e urgenti nel rispetto dei principi generali dell'ordinamento, al fine di prevenire e di eliminare gravi pericoli che minacciano l'incolumità pubblica e la sicurezza urbana. I provvedimenti di cui al presente comma sono preventivamente comunicati al Prefetto anche ai fini della predisposizione degli strumenti ritenuti necessari alla loro attuazione. 4-bis. Con Decreto del Ministro dell'interno è disciplinato l'ambito di applicazione delle disposizioni di cui ai commi 1 e 4 anche con riferimento alle definizioni relative alla incolumità pubblica e alla sicurezza urbana.

Art. 7 Collaborazione della Polizia Municipale e Provinciale nell'ambito dei piani coordinati di controllo del territorio

1. I piani coordinati di controllo del territorio di cui al comma 1 dell'articolo 17 della L. 26/03/2001, n. 128, che possono realizzarsi anche per specifiche esigenze dei comuni diversi da quelli dei maggiori centri urbani, determinano i rapporti di reciproca collaborazione fra i contingenti di personale della polizia municipale e provinciale e gli organi di Polizia dello Stato. 2. Con decreto da adottare entro tre mesi dalla data di entrata in vigore della legge di conversione del presente decreto, il Ministro dell'interno, di concerto con il Ministro della giustizia, con il Ministro dell'economia e delle finanze e con il Ministro della difesa, determina le procedure da osservare per assicurare, nel corso dello svolgimento di tali piani coordinati di controllo del territorio, le modalità di raccordo operativo tra la Polizia Municipale, la Polizia Provinciale e gli organi di Polizia dello Stato.)

Art. 8 Accesso della Polizia Municipale al Centro elaborazione dati del Ministero dell'interno

1. All'art. 16-quater del D.L 18/01/1993, n. 8, convertito, con modificazioni, dalla L. 19/03/1993, n. 68, sono apportate le seguenti modificazioni: (a) al comma 1, le parole: "schedario dei veicoli rubati operante" fino alla fine del comma sono sostituite dalle seguenti: "schedario dei veicoli rubati e allo schedario dei documenti d'identità rubati o smarriti operanti presso il Centro elaborazione dati di cui all'articolo 8 della predetta legge n. 121. Il personale della polizia municipale in possesso della qualifica di agente di pubblica sicurezza può altresì accedere alle informazioni concernenti i permessi di soggiorno rilasciati e rinnovati, in relazione a quanto

previsto dall'articolo 54, comma 5-bis, del testo unico di cui al decreto legislativo 18 agosto 2000, n. 267, e successive modificazioni".

- L. 23/04/2009, n. 38 "Conversione in legge, con modificazioni, del D.L. 23/02/2009, n. 11, recante misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori"

Art. 6. Piano straordinario di controllo del territorio

(…) 7. Per la tutela della sicurezza urbana, i Comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico. 8. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza e' limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione.

- D.M. Interno del 05/08/2008 "incolumità pubblica e sicurezza urbana: definizione e ambiti di applicazione"

Per "incolumità pubblica" si intende l'integrità fisica della popolazione e per sicurezza urbana un bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità à nei centri urbani, la convivenza civile e la coesione sociale. (…) Il Sindaco interviene per prevenire e contrastare: a) le situazioni urbane di degrado o di isolamento che favoriscono l'insorgere di fenomeni criminosi, quali lo spaccio di stupefacenti, lo sfruttamento della prostituzione, l'accattonaggio con impiego di minori e disabili e i fenomeni di violenza legati anche all'abuso di alcool; b) le situazioni in cui si verificano comportamenti quali il danneggiamento al patrimonio pubblico e privato o che ne impediscono la fruibilità e determinano lo scadimento della qualità urbana; c) l'incuria, il degrado e l'occupazione abusiva di immobili tali da favorire le situazioni indicate ai punti a) e b); d) le situazioni che costituiscono intralcio alla pubblica viabilità o che alterano il decoro urbano, in particolare quelle di abusivismo commerciale e di illecita occupazione di suolo pubblico; e) i comportamenti che, come la prostituzione su strada o l'accattonaggio molesto, possono offendere la pubblica decenza anche per le modalità con cui si manifestano, ovvero turbano gravemente il libero utilizzo degli spazi pubblici o la fruizione cui sono destinati o che rendono difficoltoso o pericoloso l'accesso ad essi.

- L. 18/04/2017, n. 48 (conversione in legge del D.L 20/02/2017, n. 14 recante disposizioni urgenti in materia di sicurezza delle Città)

Ai sensi della L. 18/04/2017, n. 48 (conversione in legge del D.L 20/02/2017, n. 14 recante disposizioni urgenti in materia di sicurezza delle Città), si intende per sicurezza urbana 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

Art. 8 Modifiche al Testo Unico delle Leggi sull'ordinamento degli Enti Locali, di cui al D.Lgs 18/08/2000, n. 267

Al testo unico delle leggi sull'ordinamento degli Enti Locali, di cui al D.Lgs 18/08/2000, n. 267, sono apportate le seguenti modificazioni: a) all'art. 50: 1. al comma 5, dopo il primo periodo, e' aggiunto il seguente: "Le medesime ordinanze sono adottate dal Sindaco, quale rappresentante della comunità locale, in relazione all'urgente necessità di interventi volti a superare situazioni di grave incuria o degrado del territorio o di pregiudizio del decoro e della vivibilità urbana, con particolare riferimento alle esigenze di tutela della tranquillità e del riposo dei residenti, anche intervenendo in materia di orari di vendita, anche per asporto, e di somministrazione di bevande alcoliche e superalcoliche" (…) b) all'art. 54: 1. il comma 4-bis è sostituito dal seguente: "4-bis. I provvedimenti adottati ai sensi del comma 4 sono diretti a prevenire e contrastare le situazioni che favoriscono l'insorgere di fenomeni criminosi o di illegalità, quali lo spaccio di stupefacenti, lo sfruttamento della prostituzione, l'accattonaggio con impiego di minori e disabili, ovvero riguardano fenomeni di abusivismo, quale l'illecita occupazione di spazi pubblici, o di violenza, anche legati all'abuso di alcool o all'uso di sostanze stupefacenti". 2. Nelle materie di cui al comma 1, lettera a), numero 1, del presente art., i Comuni possono adottare regolamenti ai sensi del Testo Unico delle Leggi sull'Ordinamento degli Enti Locali, di cui al D.Lgs 18/08/2000, n. 267.

- Infine, rispetto alla disciplina comunitaria è utile richiamare i seguenti artt. del Regolamento Generale sulla Protezione Dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016:

Art. 5 Principi applicabili al trattamento di dati personali

1. I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza"); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità

Art. 6 Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o

connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

E, in subordine,

Art. 9 Trattamento di categorie particolari di dati personali

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
2.Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: (…) b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; (…).

Da quanto esposto, pur in termini non esaustivi, si evince che il sistema videosorveglianza del Comune di Valfenera integra il principio di liceità sancito dal Provvedimento dell'Autorità Garante per la protezione dei dati personali in materia di videosorveglianza del 08/04/2010 (G.U. n. 99 del 29/04/2010) e dagli artt. 5 e 6 del G.D.P.R.

Infatti, i più i più recenti interventi normativi nazionali richiamati hanno attribuito ai Sindaci e ad alle Amministrazioni Comunali specifiche competenze in materia di incolumità pubblica e di sicurezza urbana, così come le norme, anche regionali, che hanno incentivato l'uso di tali sistemi di controllo. Nel combinato disposto del D.L. n. 92/2008 (convertito nella L. 24/07/ 2008 n. 125) e del D.L. 11/2009, (convertito in L. 23/04/2009, n. 38) si ravvisano i principali interventi normativi in materia di videosorveglianza, tanto che con il cd. "pacchetto sicurezza" (il citato D.L. n. 92/2008) il legislatore ha riformulato l'art. 54 del Testo Unico delle Leggi sull'ordinamento degli Enti Locali, di cui al D.Lgs 18/08/2000, n. 267 nel senso di attribuire ai Sindaci il compito di sovrintendere alla vigilanza su tutto ciò che possa interessare la sicurezza e l'ordine pubblico e di adottare gli atti loro attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica, nonché svolgere le funzioni affidate ad essi dalla legge in materia di sicurezza e di polizia giudiziaria. Con la modifica dell'art. 54. il Sindaco, al fine di prevenire e contrastare determinati pericoli che minacciano

l'incolumità pubblica e la sicurezza urbana, può adottare con atto motivato provvedimenti, "anche contingibili e urgenti" nel rispetto dei principi generali dell'ordinamento. La nuova formulazione lascia spazio quindi ad un uso ordinario delle Ordinanze, quale strumento non necessariamente adottato per motivi di necessità ed urgenza e dotato del carattere della temporaneità.

Inoltre, sempre il D.L. 11/2009 in materia di sicurezza pubblica, di contrasto alla violenza sessuale ed atti persecutori, ha poi introdotto all'art. 6, la facoltà in capo ai Comuni di utilizzare, per finalità di tutela della sicurezza urbana, sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico, consentendo altresì la conservazione dei dati, delle informazioni e delle immagini raccolte per sette o oltre, con la formula , "fatte salve speciali esigenze di ulteriore conservazione", facendo venire meno la necessità, per i Comuni, di sottoscrivere protocolli di intesa con le Prefetture[2]. Con i recenti interventi legislativi in pratica che attribuiscono al sindaco nuovi poteri in materia di incolumità pubblica e sicurezza urbana, il legislatore ha ammesso la partecipazione diretta dei Comuni ad attività, anche operative, questioni prima strettamente riservate alle Forze dell'Ordine.

A margine di quanto esposto, si ritiene altresì integrato il principio di liceità con riferimento al D.Lgs 152/2006 "Norme in materia Ambientale" ed alla L. 24/02/1992, n. 225 e ss.mm.ii. "Istituzione del Servizio nazionale della Protezione Civile", considerando le competenze comunali in relazione ai servizi di Protezione Civile (in particolare rispetto alla gestione delle emergenze cd. "di tipo A" ed alla pianificazione locale) ed all'ambiente anche declinato nella fattispecie di igiene urbana/decoro ed attività di vigilanza in campo ambientale e gestione rifiuti, e che il sistema di videosorveglianza può trovare impiego anche per accertare i fenomeni di abbandono rifiuti e le violazione alle disposizioni relative all'igiene urbana ed alle modalità di conferimento dei rifiuti urbani ed assimilabili e per acquisire dati in forma anonima necessari alla predisposizione dell'analisi di rischio propedeutica alla redazione del piano di emergenza comunale ed alle procedure speditive in intervento.

- D.Lgs 152/2006 "Norme in materia Ambientale"

Art. 198 competenze dei Comuni

(…) 2. I comuni concorrono a disciplinare la gestione dei rifiuti urbani con appositi regolamenti che, nel rispetto dei principi di trasparenza, efficienza, efficacia ed economicità e in coerenza con i piani d'ambito (…) stabiliscono in particolare: a) le misure per assicurare la tutela igienico-sanitaria in tutte le fasi della gestione dei rifiuti urbani; b) le modalità del servizio di raccolta e trasporto dei rifiuti urbani; c) le modalità del conferimento, della raccolta differenziata e del trasporto dei rifiuti urbani ed assimilati al fine di garantire una distinta gestione delle diverse frazioni di rifiuti e promuovere il recupero degli stessi; d) le norme atte a garantire una distinta ed adeguata gestione dei rifiuti urbani pericolosi e dei rifiuti da esumazione ed estumulazione (…); e)

[2] Prima di tali interveti normativi, non rientrando la sicurezza pubblica nella funzione istituzionale dei Comuni, la legittimità delle riprese effettuate era sempre stata collegata alle competenze "tradizionali" dei Comuni il cui esercizio era attribuito al Corpo di Polizia Municipale ovvero il controllo del traffico, la prevenzione degli atti vandalici in determinate zone, ma mai attività di indagine e di tutela della sicurezza urbana.

le misure necessarie ad ottimizzare le forme di conferimento, raccolta e trasporto dei rifiuti primari di imballaggio in sinergia con altre frazioni merceologiche, fissando standard minimi da rispettare (…).

- L. 24/02/1992, n. 225 e ss.mm.ii. "Istituzione del Servizio Nazionale della Protezione Civile".
- D.Lgs 02/01/2018, n. 1 "Codice della Protezione Civile"

Art. 15 Competenze del Comune ed attribuzioni del Sindaco (L. 24/02/1992, n. 225)

(…) 3. Il Sindaco è autorità comunale di Protezione Civile. Al verificarsi dell'emergenza nell'ambito del territorio comunale, il sindaco assume la direzione dei servizi di emergenza che insistono sul territorio del Comune, nonché il coordinamento dei servizi di soccorso e di assistenza alle popolazioni colpite e provvede agli interventi necessari dandone immediata comunicazione al prefetto e al Presidente della Giunta Regionale (…). 3-bis. Il Comune approva (…) il piano di emergenza comunale previsto dalla normativa vigente in materia di Protezione Civile (…). 3-ter. Il Comune provvede alla verifica e all'aggiornamento periodico del proprio piano di emergenza comunale (…).

Art. 6 (D.Lgs 02/01/2018, n. 1) Attribuzioni delle autorità territoriali di protezione civile (Art. 1-bis, comma 2, legge . 24/02/1992, n. 225; Art. 5, comma 5, D.L. 343/2001, conv. in L. 401/2001)

1. Nel rispetto delle direttive adottate ai sensi dell'articolo 15 e di quanto previsto dalla legislazione regionale, i Sindaci (…) in qualità di autorità territoriali di Protezione Civile, esercitano le funzioni di vigilanza sullo svolgimento integrato e coordinato delle medesime attività da parte delle strutture afferenti alle rispettive amministrazioni. Le autorità territoriali di protezione civile sono responsabili, con riferimento agli ambiti di governo e alle funzioni di competenza e nel rispetto delle vigenti normative in materia (…)

Comuni e sicurezza urbana (considerazioni generali disciplina applicabile)

Rispetto al regime giuridico degli impianti di videosorveglianza installati da Enti locali "L'art.38, comma 3, del D.L. 16/07/2020 n. 76, convertito in L. 11/09/2020, n. 120, ha previsto l'equiparazione del regime di installazione degli impianti in capo agli Enti Locali a quello – più favorevole – previsto per le amministrazioni statali. La disposizione citata prevede infatti che l'installazione e l'esercizio di sistemi di videosorveglianza come identificato all'art. 5, comma 2, lettera a), del D.L. 20/02/2017, n.14, convertito, in L 18/042017, n.48, da parte degli Enti Locali, possa essere considerata attività libera e non soggetta ad autorizzazione generale di cui agli artt. 99 e 104 del D.Lgs 01/08/2003, n.259, in base agli effetti dispiegati dai sistemi di ripresa in ambito pubblico ed area urbana, anche se installati dagli Enti locali, per il controllo del territorio e la prevenzione e repressione di illeciti.

Con riferimento alla citata L. 23/04/2009, n. 38 "Conversione in legge, con modificazioni, del D.L. 23/02/2009, n. 11, recante misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori" che consente ai Comuni di far uso di sistemi di videosorveglianza al fine di prevenzione dei reati e controllo del territorio, si è ampiamente discusso sulla sostanziale "estensione" agli stessi Comuni, pur di norma nel perimetro della Polizia Locale, di finalità precedentemente di stretta competenza delle autorità di polizia. Per i Comuni, quindi, non parrebbe più sussistere il limite della finalità delle riprese, estendendo il trattamento dei dati personali con sistemi di videosorveglianza allo scopo generale di "tutela del territorio", rendendo ammissibile il trattamento anche ai fini di controllo delle violazioni (quali le violazioni in campo ambientale e abbandono (conferimento rifiuti, o i cd. "molteplici usi").

Il tema in discussione – di chiara rilevanza – è quindi se per gli impianti utilizzati dai Comuni che sono destinati alla tutela della sicurezza urbana le regole in materia di protezione dei dati personali siano dettate dalla Direttiva 2016/680 (Direttiva Polizia) recepita con D.Lgs 18/05/2018, n. 51 e non (unicamente) dal Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016.

Infatti, il quadro complessivo che si è delineato negli ultimi anni, parrebbe consentire ai Comuni, a seguito della sottoscrizione di appositi patti per la sicurezza, di garantire l'accesso consolidato i propri sistemi di videosorveglianza anche alle Questure e ai Comandi Provinciali Carabinieri che, sotto il mero "profilo investigativo" assolvono nel migliore dei modi i loro compiti conservando le immagini per un periodo significativamente esteso. In tal senso, il D.Lgs 18/05/2018, n. 51, specificamente dedicato alla tutela dei dati personali per i soggetti che svolgono indagini, compresa la Polizia Locale, deroga abbondantemente ad alcuni principi fondamentali del dal Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, sia dilatando i tempi di conservazione dei dati che affievolendo i diritti degli interessati (che, a mero titolo esemplificativo, si vedono sottrarre la possibilità di proporre l'opposizione al trattamento prevista ordinariamente dall'art. 21 del G.D.P.R.).

Si ritiene che le basi giuridiche che rendono legale il trattamento sono costituite dalla L. 23/04/2009, n. 38 "Conversione in legge, con modificazioni, del D.L. 23/02/2009, n. 11, art. 6, commi 7 e 8, sulla utilizzabilità, da parte dei Comuni, di sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana, dalla Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27/04/ 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, dal G.D.P.R., art. 6, sulle condizioni di liceità del trattamento dei dati personali, dal D.Lgs. 196/2003 (integrato con le modifiche introdotte dal D.Lgs. n. 101/2018) art. 2-octies, sui principi relativi al trattamento di dati relativi a condanne penali e reati e dal Regolamento Comunale per l'utilizzo di impianti di videosorveglianza del territorio.

In tale senso, di supporto il Provvedimento del 26/02/2020 dell'Autorità Garante (doc. web n. 9309458) che richiama la citata disciplina normativa e in particolare, pur applicandosi al caso di specie 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 (art. 4 D.L. n. 14/2017).

3.3. VALUTAZIONE DELLA NECESSITÀ E PROPORZIONALITÀ DEI TRATTAMENTI IN RELAZIONE ALLE FINALITÀ

Come indicato nel paragrafo precedente il trattamento dati personali effettuato tramite i sistema di videosorveglianza in adozione da parte del Comune di Valfenera fonda le proprie basi giuridiche sulla L. 23/04/2009, n. 38 "Conversione in legge, con modificazioni, nel D.L. 23/02/2009, n. 11, art. 6, commi 7 e 8, sulla utilizzabilità, da parte dei Comuni, di sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana, sulla Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27/04/ 2016, nel G.D.P.R., art. 6, sulle condizioni di liceità del trattamento dei dati personali, oltre che sul D.Lgs. 196/2003 (integrato con le modifiche introdotte dal D.Lgs. n. 101/2018) art. 2-octies, sui principi relativi al trattamento di dati relativi a condanne penali e reati e dal Regolamento Comunale per l'utilizzo di impianti di videosorveglianza del territorio.

Occorre tuttavia approfondire la sussistenza, nel concreto, del principio di necessità e proporzionalità rispetto alla progettazione del posizionamento dei punti di ripresa, strettamente connesso al grado di rischio effettivo, che avrebbe dovuto escludere dalla videosorveglianza quelle aree che non sono soggette a pericoli o per le quali non ricorre un'effettiva esigenza di controllo o di deterrenza.

L'utilizzo di sistemi di ripresa è stato previsto solo quando altre misure meno "invasive" sono state ponderatamente valutate insufficienti o concretamente inefficaci o inattuabili.

A partire dal documento risalente all'anno 2019 riconducibile al progetto denominato "messa in sicurezza dell'area urbana mediante l'ampliamento dei sistema di videosorveglianza" (progetto esecutivo) e relativo ai sistemi di ripresa già esistenti, si evince che l'Amministrazione si è posta l'obiettivo di mettere in sicurezza le zone del territorio comunale definite "sensibili" agli atti criminosi e che "mira a dare ai soggetti competenti (Polizia Municipale, Forze dell'Ordine, Vigilanza privata ..) tutti gli strumenti necessari per poter intervenire non solo post-evento ma anche, eventualmente, in tempo reale durante l'accadimento del fatto".

La definizione dell'architettura di sistema (non solo in termini di numero di telecamere, posizionamento ed aree assoggettate a ripresa, ma, in generale, in termini di necessità ed efficacia delle riprese video) ha tenuto conto di una pluralità di fattori quali l'impatto della

videosorveglianza sulla percezione di sicurezza dei cittadini riferita al contesto economico e culturale locale e la coerenza con le strategie locali di contrasto alla “criminalità” rispetto agli ordinari strumenti di controllo concretamente attuabili, sempre rispetto al “limitato” contesto locale .

Pur se non compiutamente esplicitato negli atti disponibili l’Amministrazione procedente ha supportato le proprie scelte con un’analisi dei bisogni di sicurezza nell’ambito dei lavori del Tavolo Provinciale per l’Ordine e la Sicurezza Pubblica, che ha consentito di acquisire tutti gli elementi relativi alle condizioni fisiche ed al la sicurezza della zona in esame individuando i luoghi specifici di intervento sulla base delle problematiche emerse negli ultimi anni, in particolare rispetto al corretto utilizzo degli spazi pubblici e di limitati episodi di furti o danneggiamento, tenendo conto anche degli altri fattori che incidono sulle condizioni di insicurezza quali degrado sociale e ambientale, percezione della sicurezza, atti di vandalismo e devianza … e di valutare la videosorveglianza, quindi, come la risposta più adeguata per i problemi riscontrati, per se altamente invasiva della sfera di libertà dei cittadini.

La valutazione, anche in ossequio al principio di necessità, si presuppone abbia tenuto conto anche di questi elementi di criticità:

- debole potere deterrente della videosorveglianza, maggiore utilità per le attività d’indagine conseguenti alla segnalazione di un reato o di un fatto rilevante;
- inefficacia della videosorveglianza nell’affrontare problematiche connesse ai fenomeni di disordine urbano, pur considerando la natura di “piccolo comune” ed il contesto socio-economico locale;
- maggiore efficacia della videosorveglianza in alcune tipologie di luoghi (aree circoscritte e delimitate), di maggiore difficoltà valutarne l’efficacia in luoghi aperti;
- tempi di realizzazione e, soprattutto, di aggiornamento e gestione degli impianti e di formazione/addestramento del personale da valutare rispetto al dispiego di personale dedicato alle medesime finalità

Non si hanno riscontri diretti, se non una generica indicazione contenuta nella premessa descrittiva della documentazione progettuale in merito alla necessità dell’Amministrazione preoccuparsi della sicurezza dei cittadini ed alla tutela del proprio territorio, di una valutazione critica rispetto alla natura dei fenomeni criminoso che caratterizzano il territorio di Valfenera e neppure rispetto all’adeguatezza dell’intervento per ogni area ed ogni posizionamento, se non per quanto demandato al Tavolo Provinciale per l’Ordine e la Sicurezza Pubblica, in merito:

- alla probabilità di verificarsi di un di un reato o di un fatto rilevante;
- alle conseguenze di una mancata registrazione/monitoraggio di un reato o di un fatto rilevante;
- alla eventuale priorità di un reato o di un fatto rilevante da monitorare;

- all'eventuale impiego di metodi di "controllo" del fenomeno che porta al reato o al fatto rilevante alternativi (o più convenienti in termini di rapporto costi/efficacia), come per esempio il potenziamento dell'illuminazione pubblica, l'adozione di sistemi anti intrusione o sistemi di allarme, la presenza fisica di agenti o personale preposto, l'installazione di barriere fisiche ….

Il quadro che è emerso dall'analisi sommariamente descritta è quello di un territorio che non presenta emergenze specifiche, ma piuttosto la necessità di disporre, nella prima ipotesi progettuale realizzata, di sistemi tecnologici invasivi ma in numero limitato e tuttavia sufficiente a garantire la sorveglianza mirata di specifiche aree caratterizzate, talune, da un forte passaggio veicolare come nel caso degli accessi al concentrico oltre che da puntuali situazioni di rischio potenziale in determinati periodi della giornata o in quanto luoghi di aggregazione e di fruizione .

Sulla scorta di quanto sopra i posizionamenti delle telecamere hanno quindi privilegiato i punti in cui è maggiormente emersa, ad opinione dell'Amministrazione, la necessità di disporre un "presidio" localizzato del territorio a causa dell'inefficacia degli strumenti ordinariamente disponibili sia in relazione alla tipologia di evento atteso che alla frequenza

In termini generali, gli apparati di ripresa devono essere predisposti in modo tale da limitare il più possibile l'angolo visuale all'area effettivamente da "proteggere" o monitorare, ai beni da tutelare, evitando, compatibilmente con le prestazioni delle telecamere indicate a progetto e che potranno essere successivamente adottate, in particolare nel caso di quelle tipo dome brandeggiabili-"speed dome", per le quali è indispensabile evitare la ripresa "di default" di luoghi circostanti e di particolari non rilevanti (in ossequio al principio di non eccedenza nella trattamento dei dati personali).

Qui a seguito si riproduce il campo di visuale effettivo consentito dai sistemi di ripresa così come previsti a progetto e ad oggi già operative:

Fig. 1 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc fissa Via Scanagatti “casetta acqua”)

Fig. 2 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc ocr Via Scanagatti “casetta acqua”)

Fig. 3 - dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc fissa incrocio Piazza Tommaso Villa, Piazza Roma e Via Natale Fiorito ”piazza comunale”)

Fig. 4 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc fissa Largo Conte Quirico)

Fig. 5 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc fissa Strada Villata Via del Buon Consiglio)

Fig. 6 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc ocr Strada Villata Via del Buon Consiglio)

Fig. 7 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc fissa Via Vittorio Veneto Via Villanova))

Fig. 8 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc fissa Piazza Tommaso Villa)

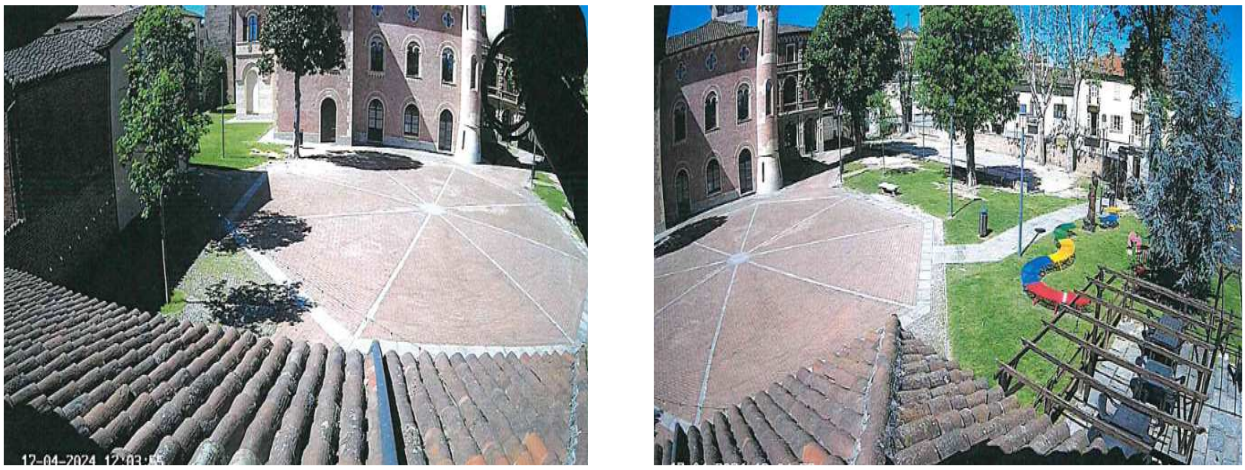

Fig. 9 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc fisse Parco Comunale)

Fig. 10 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc fissa Strada per Dusino San Michele – Stabilimento COR Tubi)

Fig. 11 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc ocr Strada per Dusino San Michele – Stabilimento COR Tubi)

Fig. 12 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc fissa Via San Lorenzo)

Fig. 13 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc fissa Strada Isolabella)

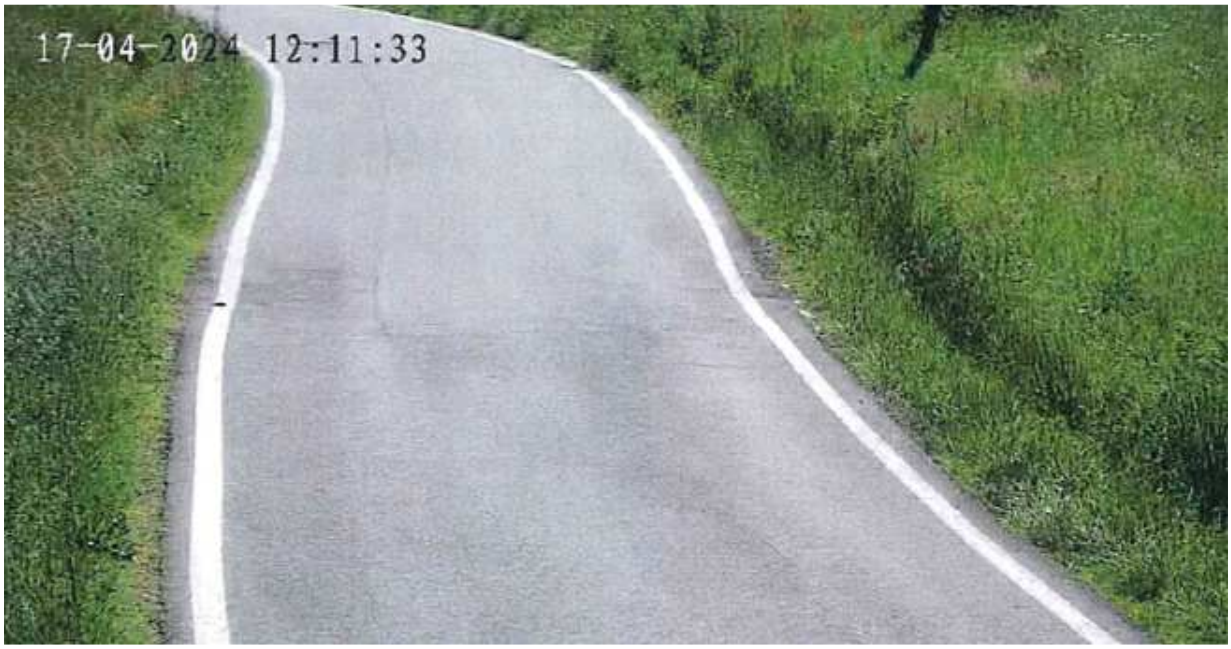

Fig. 14 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc ocr Strada Isolabella)

Fig. 15 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc fissa Cimitero)

Fig. 16 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc fissa Cimitero Fraz. Villata)

Fig. 17 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc fissa Bricco Visconti)

Fig. 18 – dettaglio area pubblica soggetta a controllo con sistemi di ripresa
(tlc fissa Parco della Rimembranza)

Rispetto invece, al progetto denominato “realizzazione di opere per la messa in sicurezza dell’area urbana mediante l’ampliamento dell’impianto di videosorveglianza” datato dicembre 2021 che prevede la fornitura di telecamere di contesto (n. 15) e lettura targhe (n. 10) per finalità di monitoraggio delle aree a rischio del territorio comunale, occorre sottolineare che lo stesso prevede un significativo incremento delle aree sottoposte a controllo, e in particolare:

denominazione sistema di ripresa	Ubicazione	tipologia
Via Villanova/Vittorio Veneto	Incrocio via Villanova/via Vittorio Veneto	1 Contesto 1 Lettura targhe
Via Villanova/Vittorio Veneto	Incrocio via Villanova/via Vittorio Veneto	1 Contesto 1 Lettura targhe
Via Villanova	Via Villanova 42	1 Contesto 1 Lettura targhe
Via S. Andrea	Via S. Andrea 2	1 Contesto
Via Gorizia	Via Gorizia	1 Contesto
Largo Conte Quirico	Largo Conte Quirico	1 Lettura targhe
Via Diaz	Via Diaz	1 Contesto
Piazza Giardinetto	Piazza Giardinetto	1 Contesto
Comune	Piazza Tommaso Villa	1 Contesto
Via Berardi/San Sebastiano	Incrocio via Gino Berardi/via San Sebastiano	1 Lettura targhe
Via Europa	Via Europa	1 Contesto
Campo sportivo	Piazza Marchesato di Saluzzo	1 Contesto
Strada Borgarella	Strada Borgarella	1 Contesto 1 Lettura targhe
Fraz. San Sebastiano	Fraz. San Sebastiano	1 Contesto 1 Lettura targhe
Fraz. Valsuolo	Fraz. Valsuolo	1 Contesto 1 Lettura targhe
Largo Don Gino Bosticco	Largo Don Gino Bosticco	1 Contesto
Fraz. Villata	Fraz. Villata	1 Contesto
Pilone Madonna del Buon Consiglio	Pilone Madonna del Buon Consiglio	2 Lettura targhe

Rispetto ai principi applicabili al trattamento di dati personali previsti dal Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, non vi è dubbio che gli ulteriori trattamenti effettuati in termini di mole di informazioni (immagini) acquisite rientrino in un ambito di trattamento lecito, corretto e trasparente nei confronti dell'interessato ed effettuato per finalità determinate, esplicite e legittime.

Corre tuttavia l’obbligo di valutare in maniera più approfondita se l’incremento dell’ampiezza del trattamento in termini di nuovi e diversi punti di ripresa sia rispettoso del principio di minimizzazione e limitazione delle finalità, tenendo conto che, in relazione ai luoghi di

installazione delle telecamere, saranno potenzialmente interessati tutti i soggetti ed i mezzi di trasporto che transitano nel concentrico.

Pur considerando i limiti delle risorse concretamente disponibili **occorre meglio motivare i presupposti sottesi alla specifica politica di controllo del territorio, che consente all'Amministrazione l'utilizzo degli impianti comunali di videosorveglianza ai fini di prevenzione e repressione di atti delittuosi in aderenza a quanto previsto dal D.M. Interno del 05/08/2008 e dalla L. 18/04/2017, n. 48 (conversione in legge del D.L 20/02/2017, n. 14 recante disposizioni urgenti in materia di sicurezza delle Città) che definiscono e circoscrivono gli ambiti di applicazione della "incolumità pubblica e della sicurezza urbana" ed i conseguenti interventi del Sindaco**.

Un cenno a parte merita, invece, il previsto utilizzo del sistema di sistema videosorveglianza del Comune di Valfenera per quanto rientra potenzialmente nelle cd "plurime finalità dell'Ente Locale"[3], che comprendono anche la tutela varie matrici ambientali ed il decoro urbano (nel caso specifico il contrasto ai fenomeni di abbandono rifiuti), tenendo conto che, come sopra illustrato, alcuni sistemi di ripresa sono collocati in modo da riprendere le aree in cui sono posizionati i contenitori stradale per la raccolta dei rifiuti urbani.

Negli ultimi anni, nonostante la ormai capillare articolazione del servizio pubblico di igiene urbana, si è assistito all'intensificarsi del fenomeno dell'abbandono rifiuti sul territorio comunale. Le osservazioni condotte hanno portato ad identificare due sostanziali differenti caratteristiche che tipizzano l'abbandono rifiuti: infatti, il fenomeno è rappresentato sia da abbandoni estemporanei e non legati a specifiche caratteristiche del territorio che dall'accumulo di rifiuti, urbani e speciali, in luoghi ben precisi del territorio, isolati e di norma poco frequentati, ad opera di utenze domestiche o imprese. Diverso, invece, è il caso dei rifiuti che vengono abbandonati nei pressi dei contenitori stradali o depositati fuori degli orari previsti per l'esposizione, su cui si può meglio intervenire attraverso accorgimenti tecnici legati alle modalità di conferimento o con l'attività ispettiva in capo al gestore del servizio pubblico di raccolta.

Rispetto all'accumulo di rifiuti in specifiche zone del territorio, l'installazione di sistemi di videosorveglianza potrebbe raggiungere l'obiettivo di costituire un valido deterrete per comportamenti scorretti e, in ogni caso, uno strumento per accertare le violazioni legate alla scorretta gestione dei rifiuti

In via preliminare, risulta utile specificare anche in questo documento che non si ravvisano cause ostative specifiche all'impiego di sistemi di videosorveglianza per esigenze di carattere "ambientale" o riconducibili alla violazione della disciplina sulla raccolta e gestione dei rifiuti. Una tale impostazione è stata confermata dall'Autorità Garante per la protezione dei dati personali che, in sede di relazione annuale 2014 (presentata formalmente in data 23/06/2015) ha

[3] Regione Piemonte, Assessorato alla Promozione della Sicurezza ed alla Polizia Locale, Quaderno di aggiornamento n. 47 "La videosorveglianza e gli Enti Locali", Cap. IV "Le pronunce del Garante", Regione Piemonte 2011.

sintetizzato le posizioni espresse in merito al trattamento di dati personali effettuato tramite telecamere in ambito pubblico, in particolare da parte dei Comuni in sede di controlli di tipo amministrativo. In particolare, l'Autorità ha sostenuto che possono essere lecitamente utilizzati sistemi di videosorveglianza anche per accertare l'utilizzo anomalo di aree impiegate come punti di raccolta di rifiuti o per accertare il rispetto delle disposizioni relative al conferimento rifiuti al ciclo pubblico di raccolta.

Il Provvedimento dell'Autorità Garante per la protezione dei dati personali in materia di videosorveglianza del 08/04/2010 (G.U. n. 99 del 29/04/2010), al punto 5.2, prevede che: "l'utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi. Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (…)", sostituendo parzialmente quella del 29/04/2004 che, invece, considerava illecita e da effettuare con altri strumenti la ripresa a mezzo di telecamera volta ad accertare solo infrazioni amministrative rispetto a quest'ultima fattispecie.

Rispetto alla motivazione che deve supportare gli atti che potranno portare all'adozione di sistemi di videosorveglianza finalizzati anche a prevenire il fenomeno dell'abbandono rifiuti, possono individuarsi due differenti approcci che si collocano vicendevolmente agli antipodi: l'uno, secondo il quale non saranno e non sono mai concretamente attuabili diverse misure efficaci per controllare e contrastare la scorretta gestione dei rifiuti, l'altro secondo il quale, invece, il controllo potrà essere sempre effettuato migliorando "l'organizzazione" della macchina comunale (istituzione/potenziamento del servizio di Polizia Locale, introduzione di controlli da parte degli addetti al servizio di raccolta rifiuti, apposizione di barriere fisiche …).

Si ritiene che, seguendo un ragionamento il più possibile equilibrato e contemperando le esigenze di tutela ambientale con le oggettive difficoltà organizzative, nella maggior parte delle situazioni riscontrate possa ricorre il requisito dell'inefficacia o dell'inattuabilità delle "altre misure" citate dall'Autorità Garante per la protezione dei dati personali. Infatti, per garantire una minima efficacia di un intervento almeno dissuasivo occorrerebbe sottoporre a controllo pur limitate porzioni di territorio ma con frequenza elevata ed anche in orario notturno, occorrerebbe "intercettare" ed identificare i trasgressori nel momento dell'abbandono o procedere all'esame puntuale dei rifiuti rinvenuti al fine di acquisire eventuali elementi che possano consentire in qualche modo di risalire anche presuntivamente all'autore dell'illecito (quali ricevute, fatture, corrispondenza ..). Condizione, questa, difficilmente attuabile per un piccolo Comune sia considerate sia le concrete e limitate possibilità operative del Servizio di Polizia Locale dell'Unione che l'assenza di un'attività di "monitoraggio ambientale" previsto nel contratto di servizio facente capo al gestore del servizio di raccolta e trasporto rifiuti urbani. Rispetto, invece, all'apposizione di barriere fisiche, si può spaziare dalla mera installazione di cancelli o sbarre a chiusura della viabilità o all'innalzamento di barriere in punti specifici, con tutti gli evidenti limiti dell'intervento:

basti pensare, a titolo di esempio, ai tratti viari, anche interpoderali, che non possono essere interdetti ai titolari o ad un numero così elevato di aventi diritto tale da rendere inopportuna la misura di tutela oppure all'interdizione all'so delle aree di sosta stradali che ne vanificherebbero la funzione sotto il profilo della sicurezza della circolazione.

Rispetto alla motivazione che deve supportare gli atti che potranno portare all'adozione di sistemi di videosorveglianza finalizzati anche a prevenire il fenomeno dell'abbandono rifiuti, occorre individuare quindi il corretto punto di equilibrio tra l'impiego di forme di monitoraggio invasive quali proprio le riprese video su vasta scala e misure di controllo "tradizionali" riconducibili, come anticipato, a servizi mirati della Polizia Locale o degli addetti al servizio di raccolta rifiuti oltre che all'apposizione di barriere fisiche.

Nel caso del Comune di Valfenera, il contratto di servizio per la raccolta e trasporto di rifiuti garantisce, a partire dall'ottobre 2024, l'attività di monitoraggio del territorio tramite "ispettori ambientali" in capo al gestore, per cui il requisito dell'inefficacia o dell'inattuabilità delle "altre misure" citate dall'Autorità Garante Nazionale parrebbe gradualmente scemare, per cui il sistema videosorveglianza quale strumento legittimo di trattamento dati è supportato da uno dei presupposti di necessità e proporzionalità sottesi all'azione dei soggetti pubblici solo quando finalizzata alla prevenzione di fenomeni di abbandono rifiuti sul territorio comunale in specifici e particolari punti o condizioni o per l'effettuazione di "campagne temporanee" di monitoraggio.

Oltre a quanto possibile monitorare con le telecamere fisse che andranno ad inquadrare, pur incidentalmente, alcuni punti di presa dei rifiuti urbani, tenendo conto che, per quanto noto, il Comune di Valfenera potrà quindi individuare alcune limitate aree isolate del territorio caratterizzate da frequenti abbandoni di rifiuti o scorretto conferimento degli stessi da parte degli utenti, il titolare potrà valutare l'opportunità di effettuare campagne di monitoraggio anche con strumenti mobili nel rispetto di tutte le garanzie richieste dal Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 e dalle pertinenti pronunce dell'Autorità Garante Nazionale, da interrompere allorquando il fenomeno risulti cessato o quantomeno rientrato in limiti "fisiologici.

Pertanto, Il sistema videosorveglianza del Comune di Valfenera può considerarsi a tutti gli effetti lo strumento idoneo a perseguire il fine dettato della norma invocata e la sua adozione si fonda sui uno dei presupposti di necessità e proporzionalità sottesi all'azione dei soggetti pubblici anche quando finalizzata alla prevenzione di fenomeni di abbandono rifiuti sul territorio comunale[4], qualora impiegato con i limiti sopra descritti e meglio circostanziati nelle conclusioni.

Sotto il profilo più specifico delle caratteristiche e della "qualità formale" dei dati trattati e della sua relazione con il principio di necessità**,** il sistema videosorveglianza del Comune di Valfenera è progettato per escludere ogni uso superfluo dei dati personali (immagini) ed evitare eccessi e ridondanze, ed il sistema informativo e il relativo programma informatico ad esso riconducibile è

[4] Quirico F, relazione (int.) 21/07/2016

conformato in modo da cancellare periodicamente e automaticamente i dati eventualmente registrati, con il termine di conservazione fissato in 7 giorni.

Tuttavia, rispetto al "dato personale/immagine" ed alla sua peculiarità ed ai fini del presente documento, occorre approfondire alcuni aspetti. Procedendo in via schematica:

- come evidente, l'immagine acquisita attraverso il sistema videosorveglianza del Comune di Valfenera si configura come dato personale in quanto rappresenta un'informazione concernente una persona fisica identificata o identificabile, anche indirettamente, oppure una o più informazioni riguardanti una persona la cui identità è nota o può comunque essere accertata mediante informazioni supplementari", come già previsto dalla della Convenzione del Consiglio 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale [5] e confermato dal G.D.P.R. ("dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale).
- per identificazione si intende la possibilità di individuare, riconoscere e distinguere un individuo da qualsiasi altro soggetto o del medesimo all'interno di una categoria e, di conseguenza, i dati si considerano personali solo se consentono l'identificazione dell'individuo oppure se le informazioni descrivono l'individuo in modo tale da consentirne l'identificazione anche acquisendo altri dati;
- anche le targhe dei veicoli possono essere considerate un dato personale in quanto, pur potenzialmente, possono essere ricondotte ad un individuo e renderlo identificabile oltre che definirne posizione e spostamenti, (in tal senso Cass. Pen. 02/12/2011, n. 4494 "anche il numero di targa del veicolo, a nulla rilevando che esso sia visibile a tutti quando l'auto circola per strada. Ciò che rileva, ovviamente non è il numero in sé, ma il suo abbinamento ad una persona");
- il dato personale costituito da un'immagine, più di altri, parrebbe un concetto dinamico che va sempre riferito e analizzato nel proprio contesto verificando, caso per caso, se le "informazioni" che l'immagine trasmette possano essere concretamente utilizzare per l'identificazione di un individuo;
- come accennato in precedenza in fase di progettazione del trattamento dati al sistema di videosorveglianza del Comune di Valfenera non è stata attribuita l'attitudine o la funzionalità tecnica per procedere all'identificazione automatica delle persone ma, come detto, a raccogliere e registrare e custodire, per un tempo limitato, dati anonimi;

[5] Convenzione del Consiglio 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale; art. 2 dati a carattere personale» significa ogni informazione concernente una persona fisica identificata o identificabile ("persona interessata").

- si considera anonimo, in termini generali ed anche intuitivamente, il dato che, in origine o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- l'Autorità Garante per la protezione dei dati personali, pur in termini non recenti, ha avuto modo di pronunciarsi sul tema, e precisamente:
  - 23/01/1998, in Bollettino n. 3, pag. 24 [doc. web n. 39568]
    "L'informazione originariamente non associabile ad uno specifico interessato (c.d. dato anonimo) può divenire "dato personale" ex art. 1 della L. n. 675/1996 allorché, attraverso una successiva operazione di collegamento ad informazioni di diversa natura, risulti comunque idonea a rendere identificabile un soggetto. Ne consegue che, ai sensi dell'art. 27, comma 3 della legge n. 675/1996, in mancanza di specifiche norme di legge o di regolamento, non può ritenersi consentita la comunicazione a privati, da parte di un soggetto pubblico, di dati statistici apparentemente anonimi, qualora il campione dei dati da analizzare, benché richiesto per scopi scientifici e di ricerca, per genere e consistenza numerica, consenta di risalire ai diretti interessati".
  - 14/06/2001, in Bollettino n. 21, pag. 43 [doc. web n. 41782]
    "Non violano le disposizioni sulla protezione dei dati personali (in particolare, le prescrizioni impartite dal Garante con il Provvedimento generale del 29/11/2000) sistemi ed apparecchiature di ripresa dislocate su spiagge – a fini promozionali, pubblicitari o di informazione agli utenti – che, in ragione della distanza dal luogo ripreso o di altre caratteristiche tecniche, non consentano di identificare, anche indirettamente, gli interessati";
- le immagini acquisite ed elaborate dal sistema di videosorveglianza del Comune di Valfenera come conseguenza delle inquadrature scelte, del campo di ripresa delle telecamere e degli zoom preimpostati, non consente la rilevazione dei tratti somatici o, comunque, una chiara visione"caratteristiche del volto" di un individuo tali da renderlo immediatamente riconoscibile e, nel caso degli apparati che riprendono una scena in cui è presente del traffico veicolare, non è possibile riconoscere gli occupanti di una autovettura o di un altro veicolo e neppure, salvo un intervento diretto dell'operatore, procedere alla ad identificazioni specifiche;
- le telecamere per lettura targhe (OCR Optical Character Recognition) acquisiscono potenzialmente i dati relativi alle caratteristiche del veicolo (in termini non esaustivi, velocità, tipologia di veicolo, pannello adr, … in base alla tipologia di licenze che saranno acquisite) e ne registrano l'immagine solo limitatamente alla targa e se impostata per la rilevazione di eventuali infrazioni, oltre a specifiche targhe qualora codificate in una apposita "black list". Nel caso di rilevazioni massive dei dati (es. per la predisposizione degli scenari relativi al "rischio trasporti"), le informazioni sono acquisite sottoforma di dati numerici o alfanumerici e, pertanto, non riconducibili a veicoli identificabili e tantomeno individui (es. nr. veicoli in transito per ogni ora, velocità media di passaggio, classe di veicolo …);

- non é consentito effettuare riprese di dettaglio dei tratti somatici delle persone che non siano funzionali alle finalità istituzionali dell'impianto attivato o al di fuori dell'ambito delle attività di prevenzione o accertamento dei reati che possono essere disposti dall'Autorità Giudiziaria o disciplinati in specifici protocolli;
- l'eventuale identificazione di un individuo può avvenire in tempo differito ("sul registrato") effettuando l'estrazione delle immagini elaborate con adeguati zoom e, se necessario, attraverso l'acquisizione, anche dalle immagini stesse, di informazioni indirette utili alla collocazione certa della persona sulla scienza, solo nel caso in cui tale operazione si renda assolutamente indispensabile per l'accertamento di un reato o di un fatto rilevante;
- rispetto al previsto utilizzo del sistema di sistema videosorveglianza del Comune di Valfenera per la tutela varie matrici ambientali ed il decoro urbano (nel caso specifico il contrasto ai fenomeni di abbandono rifiuti), in relazione alle modalità di verifica delle riprese si esclude un controllo costante in remoto da parte di un operatore dedicato, in quanto l'accesso alle immagini deve avvenire in tempo differito e a seguito della verifica in loco di un avvenuto abbandono di rifiuti, oppure almeno giornalmente, qualora si propenda per controllo "slegato" dal sopralluogo in sito

Infine, corre l'obbligo di segnalare che in base all'art. 4 della L. 300/1970 e ss.mm.ii (Statuto dei lavoratori), le immagini acquisite non possono essere utilizzate per effettuare controlli sull'attività lavorativa dei dipendenti dell'Amministrazione Comunale, di altre Amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati, e neppure per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati o per finalità di promozione turistica. Tale previsione deve essere contenuta nel Regolamento per la gestione dei dati personali acquisiti mediante il sistema di videosorveglianza del Comune di Valfenera.

Alla luce di quanto sinteticamente esposto, si ritiene che le modalità di funzionamento e gestionali del sistema videosorveglianza del Comune di Valfenera, per quanto desunto dalla documentazione progettuale ed amministrativa disponibile, integri il principio di necessità così come delineato dalla più volte citata normativa comunitaria e nazionale.

3.4. LA VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI

" .. le nuove tecnologie creano rischi di inquinamento dell'ambiente delle libertà civili e politiche, per cui si rende necessario passare a tecnologie "pulite", anche attraverso una costante valutazione dell'impatto privacy[6] (Stefano Rodotà).

Come già evidenziato dal Provvedimento dell'Autorità Garante per la protezione dei dati personali in materia di videosorveglianza del 08/04/2010 (G.U. n. 99 del 29/04/2010) i sistemi dotati di videoanalisi sono da ritenersi eccedenti rispetto alla normale attività di videosorveglianza, in quanto possono determinare effetti particolarmente invasivi sulla sfera di autodeterminazione dell'interessato e, conseguentemente, sul suo comportamento.

E' del tutto intuitivo che i sistemi di videosorveglianza in spazi pubblici e in particolare in area urbana limitino il "diritto alla privacy" e che la presenza di telecamere eliminino o, meglio, riducano potenzialmente la libertà all'anonimato riconosciuta in capo ad ogni individuo. Ed è altrettanto evidente che, se da un lato il semplice fatto di "esporsi al pubblico" e di frequentare aree pubbliche comporta la rinuncia necessaria alla riservatezza, dall'altro l'essere osservati incidentalmente da estranei è situazione ben diversa dall'essere assoggettato un controllo prolungato ed intenso come quello dei sistemi di videosorveglianza, tanto più se le immagini acquisite vengono registrate e conservate per periodo più o meno lunghi. Occorre anche considerare che l'effetto invasivo della videosorveglianza può essere anche amplificato qualora i sistemi d ripresa vengano associati al "potere di controllo" dello Stato.

Inoltre – ed è quanto più interessa rispetto agli scopi del presente documento – è di evidenza anche scientifica che gli individui che sono consapevoli di trovarsi nel raggio di azione delle telecamere o di muoversi in aree potenzialmente videosorvegliate tendano a modificare i propri comportamenti non tanto perché intenti in atti scorretti o illegali ma per il semplice fatto di non voler lasciare traccia alcuna di sé o per timore di essere "giudicati" da un osservatore invisibile, o anche per il semplice timore che eventuali comportamenti possano essere mal interpretati dagli addetti al controllo.

Ancora, l'impiego di videoanalisi e la conseguente possibilità di monitorare con maggiore grado di dettaglio e discrimine anche i comportamenti degli individui può portare ad un proporzionale incremento della frequenza o della portata della modifica dei comportamenti di ciascuno.

Andrew Von Hirsch sintetizza molto bene questa criticità: "essere osservati da telecamere di videosorveglianza é come svolgere le proprie attività entro uno spazio dotato di specchio unidirezionale, con la consapevolezza che qualcuno ci sta osservando attraverso lo specchio, senza necessariamente sapere chi ci sta osservando o che cosa stia ricercando[7]".

---

[6] Panetta R, "Libera circolazione e protezione dei dati personali", Giuffrè 2006 (Prefazione S. Rodotà)

[7] Von Hirsch A. "The Ethics of Public Television Surveillance" in von Hirsch, A., Garland, D. e Wakefi Eld, A. (eds.) "*Ethical and Social Perspectives on Situational Crime Prevention",* (Hart Publishing Oxford)

In termini analoghi si è a suo tempo espresso Giovanni Buttarelli, Garante europeo aggiunto della tutela dei dati personali: "(…) il fatto di sentirsi osservati cambia il nostro comportamento. In realtà, molti di noi, se sanno di essere osservati, possono autocensurarsi. Certamente è quanto avviene in presenza di una videosorveglianza diffusa e continua. Sapere che ogni nostro movimento o gesto è monitorato da una telecamera può avere un impatto psicologico e spingerci a mutare i nostri comportamenti; il che costituisce un'interferenza nella nostra vita privata[8]".

E nello stesso modo si è anche autorevolmente espressa l'Autorità Garante francese (CNIL) – con indicazione del giugno 2020[9] – che aveva già avuto modo di sottolineare come lo spazio pubblico in cui di norma vengono installate le telecamere (anche " intelligenti" o termiche) sia un luogo in cui si esercitano numerose libertà individuali, dal diritto alla vita privata e alla protezione dei dati personali, alla libertà di muoversi, al diritto di espressione, di riunione, di manifestare, alla libertà di coscienza e di esercizio dei culti. E che "la conservazione dell'anonimato nello spazio pubblico è una dimensione essenziale per l'esercizio di tali libertà e la captazione dell'immagine delle persone in tali spazi è incontestabilmente portatrice di rischi per i diritti e le libertà fondamentali di queste ultime".

Se le circostanze descritte possono in parte essere ricondotte a sensibilità del tutto personale o alla modifica di comportamenti privi di rilevanza concreta, non è possibile escludere a priori che la presenza di un sistema di videosorveglianza possa scoraggiare i cittadini all'esercizio del diritto di libertà di espressione ed associazione negli spazi pubblici, basti pensare alla "libertà" di partecipare ad un corteo o ad una manifestazione, di avvicinarsi a "banchetti" di associazioni culturali o politiche o semplicemente di leggere un manifesto o acquistare delle pubblicazioni.

A questo si deve aggiungere – andando oltre l'aspetto meramente tecnico – che pur quando gli effetti della sorveglianza coinvolgono ampie fasce della popolazione, le decisioni circa i processi e le modalità di sorveglianza sono raramente sottoposte a una discussione o valutazione pubblica, diversamente da quanto avviene ed è formalmente previsto dalla normativa in materia ambientale (a titolo di esempio, in caso di Valutazione di Impatto Ambientale e di scelta della localizzazione di un impianto).

Se la videosorveglianza è indiscutibilmente considerata un fattore limitante della riservatezza, altrettanto indiscutibilmente non si trova traccia – anche comprensibilmente - di "parametri" oggettivi o indicazioni che possano stabilire un limite o livello predeterminato a cui riportare la

---

[8] "Legal Restrictions – Surveillance and Fundamental Rights", discorso pronunciato da Giovanni Buttarelli, Garante europeo aggiunto della tutela dei dati personali al Palazzo di Giustizia, Vienna, 19 giugno 2009 (tratto: http://efus.eu/files/2013/05/CCTV_ANGLAIS.pdf)

[9] https://www.cnil.fr/fr/cameras-dites-intelligentes-et-cameras-thermiques-les-points-de-vigilance-de-la-cnil-et-les-regles

compressione del diritto alla “privacy” rispetto all’esigenza (ed al conseguente diritto) di garantire la tutela dell’incolumità pubblica e della sicurezza urbana dei cittadini.

Il principio cardine da cui muovere è quello dell’assoluta residualità degli strumenti di videosorveglianza che, oltre a poter essere chiamati in causa solo qualora non sia possibile fare ricorso ad altri mezzi meno invasivi, devono necessariamente rispondere a requisiti di liceità, necessità, proporzionalità e trasparenza.

Nell’ottica del principio “operativo” sancito dall’art. 25 (data protection by default and by design) del Regolamento Generale sulla Protezione Dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, per le finalità del presente documento è utile determinare, pur con i limiti intrinseci del tentativo, un parametro/indice in grado di rappresentare il rischio a cui potenzialmente può essere assoggettata la riservatezza degli individui all’attivazione del sistema videosorveglianza del Comune di Valfenera, in altri e migliori termini, l’incidenza, delle attività poste in essere dal titolare sui dati personali.

Si ritiene poco significativa l’attribuzione di valori numerici alle diverse tipologie di comportamento non adottate dagli individui in presenza di videosorveglianza rispetto ad un “comportamento tipo” o valutare la “portata” della deviazione del comportamento reale dal comportamento potenziale. È invece possibile - oltre che utile, valutare il rischio per i diritti e le libertà degli interessati come lo scostamento del comportamento del titolare rispetto ai dettami tecnico/normativi in materia di protezione ei dati personali. In buona sostanza, si tenta in questo caso di “misurare” il rischio degli individui di subire trattamenti illegittimi di dati personali.
Attingendo alla metodologia sviluppata per la pianificazione di Protezione Civile pur in tempi non recenti (metodo “Augustus”) ed adattandola al contesto specifico, è possibile identificare il rischio con la possibilità che un fenomeno si verifichi e che possa causare effetti dannosi.
Il rischio è traducibile nella formula: R = P x V x E

- P = Pericolosità: probabilità che un fenomeno si verifichi
- V = Vulnerabilità: propensione a subire un danno in conseguenza del fenomeno
- E = Esposizione (valore esposto): “misurazione” (o "valore") di ognuno degli elementi soggetti a rischi.

Rispetto al contesto generale riconducibile all’attivazione del sistema videosorveglianza cittadino, considerata la difficoltà di stimare/quantificare il valore esposto e, soprattutto, a definire in maniera univoca la vulnerabilità per gli elementi non tecnologici e procedurali (propensione a subire un danno da parte dell’interessato), si può semplificare la formula già esposta in questi termini: R = f (P,D) da cui la relazione: R = P x D

- P = Pericolosità: probabilità che un fenomeno si verifichi
- D = Magnitudo (gravità) delle conseguenze del fenomeno

Si può quindi costruire, pur con le evidenti imprecisioni del caso, la seguente scala delle probabilità e la scala della magnitudo:

Scala delle probabilità		
P	*Livello di probabilità*	*Criterio di valutazione*
4	Altamente probabile	➢ L'evento può verificarsi modo indiretto o automatico rispetto ad un'azione o un comportamento ➢ Sono noti eventi già verificatesi presso le strutture in capo al titolare o altre analoghe strutture
3	Probabile	➢ L'evento può verificarsi in modo indiretto rispetto ad un'azione o un comportamento ➢ Sono noti alcuni eventi già verificatesi
2	Poco probabile	➢ l'evento può verificarsi solo in particolari circostanze ed in particolari condizioni ➢ sono noti rari eventi già verificatesi
1	Improbabile	➢ L'evento può essere provocato dal la concomitanza di più fattori poco probabili e tra loro indipendenti ➢ Non sono noti eventi già verificatesi
Scala della magnitudo		
P	*Livello delle conseguenze*	*Criterio di valutazione*
4	Gravissimo	➢ Modifica non autorizzata dei trattamenti esistenti o introduzione di nuovi trattamenti ➢ Duplicazione o creazione non autorizzata di nuovi archivi o nuove banche dati ➢ Modifica non autorizzata della direzione di ripresa e dei tempi di movimento o delle funzionalità degli strumenti di ripresa ➢ Riprese di dettaglio dei tratti somatici delle persone ➢ Riprese effettuate appositamente in proprietà private o in luoghi non pubblici e non aperti al pubblico ➢ Mancata/errata adozione dell'informativa prescritta *
3	Grave	➢ Sottrazione di dati personali a causa di accessi non autorizzati alle strumentazioni informatiche e violazione delle reti
2	Medio	➢ Posizionamento (incidentale/erroneo) dei sistemi di ripresa in modo tale da poter riprendere proprietà private o luoghi non pubblici e non aperti al pubblico ➢ Acquisizione di dati personali (immagini) in modo eccedente rispetto alle finalità dell'impianto di videosorveglianza ➢ Accessi non autorizzati alla sala di controllo ➢ Estrazione di file non protetto da parola chiave
1	Lieve	➢ Mancata cancellazione automatica dei dati acquisiti entro il periodo di tempo prestabilito ➢ Mancata/errata adozione dell'informativa prescritta *

* la "mancata adozione dell'informativa .." è stata contempla sia come danno lieve che come danno gravissimo, in quanto soggetta ad una possibile duplice valutazione: da un lato, il livello del

danno può essere considerato lieve in quanto, mancando la consapevolezza di essere ripreso, si può ragionevolmente pensare che l'interessato non modifichi i propri comportamenti oppure nel caso in cui tale mancanza assuma meramente "valore formale" (a titolo esemplificativo nel caso in cui la presenza delle telecamere sia nota e consolidata, le stesse siano chiaramente visibili, siano stati divulgati con gli ordinari mezzi di comunicazione avvisi di attivazione …). Diversamente è stata contemplata come gravissimo nel caso in cui l'informativa non collocata fisicamente prima del raggio di azione degli apparati di ripresa non abbia consentito all'interessato la modifica volontaria del proprio comportamento e neppure l'esercizio dei diritti garantiti.

Stima del rischio					
	Probabilità				
		1	2	3	4
	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
conseguenze	4	4	8	12	16

Rischio basso		Rischio medio		Rischio alto		Rischio altissimo	

La stima del rischio come appena sintetizzata deve poi ragionevolmente ricondursi alle effettive potenzialità del sistema di sistema videosorveglianza del Comune di Valfenera , costituito da sistemi di ripresa e con ridotte capacita di video analisi. La "significatività" (e il rischio associato al trattamento dei dati personali/immagini) rimanda alla concreta possibilità di identificare una persona fisica. Il rischio connesso a buona parte delle possibili violazioni al corretto trattamento dei dati personali (quali la modifica illecita della direzione di ripresa e dei tempi di movimento o delle funzionalità degli strumenti di ripresa, le riprese di dettaglio dei tratti somatici delle persone anche qualora effettuate appositamente in proprietà private o in luoghi non pubblici e non aperti al pubblico …) che possono sfociare nell'acquisizione di immagini o nella resa visione delle registrazioni, sia in sincronia che in tempo differito, deve essere necessariamente considerato (o, meglio, riconsiderato) anche in relazione alla qualità delle immagini effettivamente estratte. Come già segnalato, l'eventuale zoom non autorizzato, per buon parte delle inquadrature disponibili (considerato il posizionamento degli apparati fissi in modo tale che produrre una visione di contesto) non consente la rilevazione dei tratti somatici o, comunque, una chiara lettura delle "caratteristiche del volto" di un individuo così da renderlo immediatamente identificabile.

Infatti allo stato attuale le telecamere che saranno adottate dal Comune di Valfenera, dato l'ampio campo di ripresa degli apparati e degli zoom reimpostati come da progetto, non consente la rilevazione dei tratti somatici o, comunque, una chiara visione delle "caratteristiche del volto" di un individuo tali da renderlo immediatamente riconoscibile, anche soprattutto in modalità differita ("sul registrato"). Consente tuttavia di cogliere gli elementi principali di una scena quali il passaggio di vetture o persone (oltre che il rilievo delle targhe con i sistemi specifici di lettura).

Analogo discorso vale per la rilevazione delle targhe in presenza di campi di ripresa mediamente ampi (tipici dell'applicazione delle telecamere ad ottica fissa) e di tipo dome brandeggiabili - "speed dome" (ad oggi non adottate), possibile solo in caso di inquadratura particolarmente favorevole e con adeguato zoom operato in modalità differita ("sul registrato") o appositamente effettuato dall'operatore per motivate esigenze.

In altri limitati casi, invece, grazie a sistemi di ripresa di maggiore efficienza dovuta meramente al posizionamento degli apparati sarà possibile estrapolare un immagine sufficientemente chiara da consentire, potenzialmente, identificare la persona, pur con la necessaria presenza di ulteriori informazioni, che, come evidente, saranno acquisite solo in caso di necessità (in presenza di denunzia di reato o in caso di eventi significativi, da ricostruire con l'anali delle immagini in modalità differita "sul registrato").

Come accennato, garanzie rispetto all'ineludibilità della capacità tecnica del sistema è il divieto imposto agli operatori (che dovrà essere dal previsto dal Regolamento per la gestione dei dati personali acquisiti mediante il sistema di videosorveglianza del Comune di Valfenera) di effettuare riprese di dettaglio dei tratti somatici delle persone non strettamente funzionali alle finalità istituzionali dell'impianto attivato o al di fuori dell'ambito delle attività di prevenzione o accertamento dei reati che possono essere disposti dall'Autorità Giudiziaria o disciplinati in specifici protocolli.

Con riguardo, infine, al posizionamento dei sistemi di ripresa ed alle loro effettive potenzialità tecniche, corre l'obbligo di affrontare l'eventuale ipotesi di riprese effettuate in termini "eccedenti rispetto alle finalità del sistema", che si potrebbe verificare nel caso in cui la telecamera riportasse nell'inquadratura anche "aree private" quali balconi, cortili, autorimesse …

Una simile casistica è stata invero affrontata dall'Autorità Garante per la protezione dei dati personali con pronuncia, pur datata, del 04/10/2007 (Videosorveglianza comunale e riprese all'interno di abitazioni private - doc. web n. 1457505), in cui è stato osservato, nel caso concreto che gli operatori potessero spostare le telecamere in tutte le direzioni ed effettuare zoom riprendendo parti non pertinenti rispetto agli scopi e alle finalità dell'installazione, quali finestre di appartamenti privati e rendere così identificabili i singoli cittadini ripresi e visibili in modo ravvicinato e che tale condizione potesse determinare un'intromissione ingiustificata nella vita privata degli interessati e forme di condizionamento nei movimenti e nei comportamenti delle persone in luoghi privati costituendo causa di legittima contestazione da parte di interessati.
Sempre nel caso di specie l'Autorità Garante per la protezione dei dati personali ha prescritto una generica limitazione, della dislocazione delle telecamere, del l'uso dello zoom, della riduzione e dell'angolo visuale degli apparati in modo da escludere ogni forma di ripresa, anche in assenza di registrazione, di particolari non rilevanti e di spazi interni relativi a private abitazioni, anche attraverso un eventuale sistema di settaggio e oscuramento automatico delle riprese non modificabile dall'operatore.

Prendendo come riferimento tale pronuncia, si segnala quanto segue:

- l'intervento dell'Autorità garante ha come riferimento il provvedimento generale in materia di videosorveglianza del 20/04/2004 che, pur mantenendo pressoché inalterati i principi generali, deve essere necessariamente riportato all'evoluzione tecnologica dei sistemi di ripresa ed ai recenti fenomeni sociali che hanno modificato la "domanda di sicurezza" da parte dei cittadini ed anche la loro conseguente valutazione del "diritto alla riservatezza";
- il già citato D.L. 11/2009 in materia di sicurezza pubblica, di contrasto alla violenza sessuale ed atti persecutori, (convertito in L. 23/04/2009, n. 38), ha consentito ai Comuni di utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana;
- la questione dibattuta è legata ai concetti ed alle "delimitazioni" del luogo pubblico, luogo aperto al pubblico e luogo esposto al pubblico e "privata dimora, oltre al necessario bilanciamento tra le esigenze di "tutela della sicurezza" e "tutela della riservatezza";
- se con l'adozione delle garanzie del caso non insorgono particolari dubbi sulla correttezza delle riprese effettuate in luoghi pubblici o aperti al pubblico, e neppure nella "privata dimora", più sfumato è il concetto (o, meglio la sua estensione …) di luogo esposto al pubblico;
- il Gruppo di lavoro, Articolo 29, con parere 4/200410 ha precisato che la pubblicità dei luoghi può giustificare un minore livello di riserbo rispetto all'ordinario, ma non può comportare la totale privazione del diritto alla riservatezza delle persone riprese, senza tuttavia indicare la "linea di demarcazione" tra luogo pubblico o aperto al pubblico e luogo esposto al pubblico;
- in assenza di concrete indicazioni da parte del legislatore, occorre attingere alla giurisprudenza che, negli ultimi anni, si è espressa in merito alla liceità delle riprese e, in particolare, all'ammissibilità in giudizio delle "prove video" acquisite;
- pur non costituendo una posizione univoca, si ritiene significativo riferirsi a Cass. Pen., Sez. V, 14/05/2008, n. 22602. nel passaggio in cui afferma: "certamente non rientrano in simile ambito i luoghi ripresi nel caso concreto. Nel caso considerato riprese video di aree esterne ad un edificio quali ingresso, balconi e cortile), che correttamente vanno qualificati come esposti al pubblico, in quanto caratterizzati da uno spazio soggetto alla visibilità di coloro che vi si trovino. La percettibilità all'esterno fa venir meno le ragioni della tutela del luogo, anche se di proprietà dei privati (…) Tale spazio peraltro non potrebbe essere assimilato a quegli ambienti nei quali è garantita la intimità (…);
- ancora, si possono trarre elementi di giudizio utili da. Cass. Pen., Sez. Un., 28/03/ 2006, n.26795 (in tema di prove ammissibili in giudizio) in cui si definisce la "privata dimora" e si delinea i limiti all'invasività dell'azione pubblica assumendo a discrimine non tanto il luogo fisico (dimora, residenza, abitazione ..), quanto la sua relazione con l'individuo, da ricercarsi nella "stabilità", requisiti non ravvisabile nei luoghi esposti al pubblico, pur con le eventuali critiche del caso trattando la sentenza citata le riprese video effettuate all'interno di una toilette pubblica;

[10] http://www.privacy.it/grupripareri200404.htm

- interessante anche Cass. Pen., Sez. II, 10/11/ 2006, n.5591 (in tema di riprese video di aree condominiali comuni sfociate nella ripresa anche di porzioni di balconi privati), nei richiami giurisprudenziali e nel passaggio in cui afferma: “deve escludersi una intrusione, tanto nella privata dimora, quanto nel domicilio" con riferimento a videoriprese aventi ad oggetto comportamenti tenuti in spazi di pertinenza della abitazione di taluno ma di fatto non protetti dalla vista degli estranei, giacché per questa ragione tali spazi sono assimilabili a luoghi esposti al pubblico, la percettibilità all'esterno dei comportamenti in essi tenuti fa venir meno le ragioni della tutela domiciliare”.
- le riprese in area urbana, per conservare una pur minima utilità anche nella visione “sul registrato” in caso di esigenze investigative connesse alla commissione di un reato o al verificarsi di un evento significativo, non possono avere raggio di azione eccessivamente limitato (basti pensare all’inquadratura di una telecamera ad ottica fissa che riprende un via cittadina, comprese le facciate delle abitazioni prospicienti ed i relativi balconi o ingressi condominiali o ad una telecamera tipo dome brandeggiabile -“speed dome” che, ruotando anche per 360° inquadra una “panoramica” complessiva dello scenario urbano, comprese necessariamente aree private);

Da quanto verificato alcuni sistemi di ripresa che – in caso di impianto esistente e sia nel caso dell’impianto ancora da realizzare - inquadrano un’area pubblica aperta estendendo anche il proprio raggio di azione su abitazioni prospicienti

Tale posizionamento, che il progettista ha ritenuto necessario per disporre di una visione integrale dell’intera area sensibile e per poter visionare i transiti di veicoli sulla via principale, può essere mantenuto contemperando le esigenze di tutela sottese alla necessità di indagine connesse all’eventuale commissione di un reato con le legittime aspettative e diritto di riservatezza delle persone, valutando l’adozione di limitazioni concrete alla possibilità di accesso alle immagini. In ogni caso, qualora l’esigenza di riprendere il transito di veicoli sulla strada principale sia considerata ineludibile da parte del titolare, si coniglia di installare uno specifico apparato dedicato al solo monitoraggio del tratto viario interessato e di modificare di conseguenza l’inquadratura offerta dalla telecamere individuate.

Dovrà anche essere valutato se, a seguito di specifica implementazione, il sistema videosorveglianza del Comune di Valfenera consenta tecnicamente l’applicazione della cd “privacy mask” che, in situazioni particolari ed in presenza di un rischio concreto, potrà essere configurata per l’area di ripresa di una singola telecamera.

Alla luce di quanto sinteticamente argomentato, pur con i limite oggettivo dell’invasività degli strumenti tecnologici di ripresa che consentono di raccogliere e trattare una quantità rilevante di informazioni, si ritiene il sistema videosorveglianza del Comune di Valfenera sia conforme a quanto previsto dal Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, oltre che in linea con quanto prescritto dall’Autorità Garante nazionale e possa essere attribuito al trattamento un rischio basso/medio.

Infatti, le riprese effettuate dalle telecamere a servizio dell'impianto di videosorveglianza del Comune di Valfenera rispettano i principi di necessità e proporzionalità anche nel caso in cui abbiano ad oggetto luoghi esposti al pubblico, vale a dire luoghi pur "privati" ma che possano essere visti da un numero indeterminato di persone, e che, soprattutto, i potenziali rischi per i diritti e la libertà degli interessati possono essere limitati dalle richiamate indicazioni operative impartite agli addetti e dal limite temporale di conservazione delle immagini. Questo anche nel caso in cui "elementi secondari" possano teoricamente consentire l'identificazione di una persona, quali ad esempio un determinato veicolo posteggiato all'interno di un cortile o nei pressi di un'abitazione, o l'accesso ad un determinato edificio quale il complesso scolastico.

L'art. 6, comma 8, della già citata L. 23/04/2009, n. 38 "Conversione in legge, con modificazioni, del D.L. 23/02/2009, n. 11, recante misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori" prevede che, nell'ambito dell'utilizzo da parte dei Comuni di sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana, *"*la conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza sia limitata ai 7 giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione". Il trattamento dei dati personali effettuato tramite il sistema videosorveglianza del Comune di Valfenera è conforme a tale disposizione.

Rispetto invece all'analisi puntuale delle Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - Versione 2.0 adottate il 29/01/2020, è utile rilevare quanto segue, con riferimento alle condizioni operative ed all'architettura del trattamento effettuato tramite il sistema di videosorveglianza in oggetto.

Come precisato dalle citate Linee Guida, in linea di principio, ogni fondamento di diritto ai sensi dell'art. 6, par. 1, del Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 può fornire una base giuridica per il trattamento dei dati di videosorveglianza.
Infatti. Il citato art. 6, par, 1, lettera c) (trattamento necessario per adempiere un obbligo di legge al quale è soggetto il titolare del trattamento), si applica quando la normativa nazionale prevede l'obbligo di mettere in atto in sistema di videosorveglianza mentre nella pratica, le disposizioni più suscettibili di essere utilizzate sono riconducibili alla lettera f) (legittimo interesse) ed alla lettera e) (necessità al fine di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri).

In tal senso, la normativa nazionale non impone un obbligo in capo al titolare che, per assolvere alle proprie "funzioni istituzionali" ha ampia facoltà di scelta in relazione agli interventi concretamente attuabili e, di conseguenza, al trattamento dati da effettuare. Nella pratica, infatti, per il trattamento in discorso ricorrono più correttamente le statuizioni di cui alla lettera f) (legittimo interesse) ed alla lettera e) (necessità al fine di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri).

È opportuno che il trattamento effettuato in conformità a un obbligo legale al quale il titolare del trattamento è soggetto o necessario ad assolvere ad un compito svolto nell'interesse pubblico o per l'esercizio di pubblici poteri sia basato sul diritto nazionale che se il Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 non impone che vi sia un atto legislativo specifico per ogni singolo trattamento, ma spetta alla norma stabilire se il titolare del trattamento che esegue un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri debba essere una pubblica autorità o altra persona fisica o giuridica di diritto pubblico o, qualora sia nel pubblico interesse.

I legittimi interessi di un titolare del trattamento possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. Ad esempio, potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati, come nel caso della videosorveglianza su larga scala.

Posto che spetta al legislatore prevedere la base giuridica che autorizza le autorità pubbliche a trattare i dati personali, la base giuridica per un legittimo interesse del titolare del trattamento non deve valere per il trattamento effettuato da autorità pubbliche nell'esecuzione dei loro compiti.

Il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti può essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti.

Se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento, l a norma di legge può stabilire e precisare le finalità e i compiti per i quali l'ulteriore trattamento è considerato lecito e compatibile. La base giuridica dal diritto per il "primo" trattamento dei dati personali può anche costituire una base giuridica per l'ulteriore trattamento. Per accertare se la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento deve, dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario, tener conto tra l'altro di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo; della natura dei dati personali; delle conseguenze dell'ulteriore trattamento previsto per gli interessati e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto.

Sussistenza di legittimi interessi: la videosorveglianza è lecita se è necessaria per conseguire la finalità di un legittimo interesse perseguito da un titolare del trattamento o da un terzo, a meno che su tali interessi prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato (articolo 6, paragrafo 1, lettera f). I legittimi interessi perseguiti da un titolare del trattamento o da terzi possono avere natura giuridica, economica o immateriale. Tuttavia, il titolare del trattamento dovrebbe considerare che se l'interessato si oppone alla sorveglianza a norma dell'art. 21, si può procedere alla videosorveglianza di tale interessato (in questo caso della "popolazione" o, meglio, dei soggetti che in area pubblica entrano nel raggio di azione degli strumenti di ripesa) soltanto se il legittimo interesse in questione ha natura cogente e prevale sugli interessi, i diritti e le libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

In presenza di una situazione di reale rischio, la tutela della sicurezza urbana e dell'ordine pubblico può costituire un legittimo interesse con riguardo alla videosorveglianza, e si ritiene che le Linee Guida non facciano distinzione tra sfera privata e sfera pubblica (area pubblica e patrimonio pubblico).

Il legittimo interesse deve essere esistente e attuale (ossia non deve essere fittizio o ipotetico). Prima di avviare la sorveglianza è necessario che sussista una situazione di "reale difficoltà" che, nel caso di specie ed in termini generali, si ritiene sussistere nell'esigenza di garantire la sicurezza dei cittadini e la sicura fruibilità degli spazi pubblici, oltre al contrasto ai diversi fenomeni di criminalità, secondo competenze e prerogative delle diverse componenti istituzionali interessate.

Alla luce del principio di responsabilizzazione, il titolare del trattamento deve documentare gli eventi problematici in questione (data, modalità, danno...). Tali casi documentati possono costituire un solido elemento di sussistenza di un legittimo interesse. L'esistenza di un legittimo interesse e la necessità del monitoraggio devono essere oggetto di riesame periodico (ad esempio, una volta all'anno, a seconda delle circostanze).

Necessità del trattamento: i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati secondo il principio della "minimizzazione dei dati". Prima di installare un sistema di videosorveglianza, il titolare del trattamento deve sempre valutare criticamente se questa misura sia in primo luogo idonea a raggiungere l'obiettivo prefissato e, in secondo luogo, adeguata e necessaria per i suoi scopi. Si dovrebbe optare per misure di videosorveglianza unicamente se la finalità del trattamento non può ragionevolmente essere raggiunta con altri mezzi meno intrusivi per i diritti e le libertà fondamentali dell'interessato (quali, a titolo di esempio, l'adozione di misure di sicurezza alternative, il pattugliamento regolare delle diverse aree urbane ed extraurbane, una migliore illuminazione. Il titolare del trattamento deve valutare caso per caso se tali misure possano essere una soluzione ragionevole.

Occorre interrogarsi sulla necessità del trattamento anche per quanto riguarda le modalità di conservazione di elementi di prova. In alcuni casi potrebbe essere necessario utilizzare soluzioni tipo scatola nera, nelle quali il filmato viene automaticamente cancellato dopo un determinato

periodo di conservazione e vi si accede solo in caso di eventi problematici. In altre situazioni potrebbe non essere affatto necessario registrare il materiale video, essendo magari più opportuno ricorrere al monitoraggio in tempo reale. La scelta tra le due soluzioni dovrebbe anche basarsi sullo scopo perseguito. Se, ad esempio, la videosorveglianza è finalizzata alla raccolta di prove, solitamente i metodi in tempo reale non sono adatti. Talvolta il monitoraggio in tempo reale può risultare anche più intrusivo rispetto alla conservazione e alla cancellazione automatica delle registrazioni dopo un lasso di tempo limitato (ad esempio, se un operatore visualizza costantemente le immagini su monitor, questo metodo potrebbe essere più intrusivo rispetto alla conservazione diretta del materiale in una scatola nera in assenza di monitoraggio). In questo contesto occorre avere riguardo al principio della minimizzazione dei dati (articolo 5, paragrafo 1, lettera c). Occorre inoltre tenere presente la possibilità per il titolare del trattamento di avvalersi di personale di sicurezza in grado di reagire e intervenire immediatamente anziché ricorrere alla videosorveglianza.

Bilanciamento degli interessi: supponendo che la videosorveglianza sia necessaria per proteggere i legittimi interessi di un titolare del trattamento, un sistema di videosorveglianza può essere messo in funzione unicamente se sui legittimi interessi del titolare del trattamento o su quelli di terzi (ad esempio, la protezione della proprietà o dell'integrità fisica) non prevalgono gli interessi o i diritti e le libertà fondamentali dell'interessato. Il titolare del trattamento deve valutare 1) in che misura il monitoraggio incida sugli interessi, sui diritti fondamentali e sulle libertà degli individui, e 2) se ciò comporti violazioni o conseguenze negative rispetto ai diritti dell'interessato.

Decidere caso per caso: poiché il bilanciamento degli interessi è obbligatorio ai sensi del regolamento, la decisione deve essere presa caso per caso (cfr. articolo 6, paragrafo 1, lettera f)). Non è sufficiente fare riferimento a situazioni astratte o confrontare casi simili tra loro. Il titolare del trattamento deve valutare i rischi di interferenza nei diritti dell'interessato; in questo caso il criterio decisivo è l'intensità dell'intervento rispetto ai diritti e allele libertà dell'individuo. L'intensità può essere definita, tra l'altro, dal tipo di informazioni raccolte (contenuto delle informazioni), dalla portata (densità delle informazioni, estensione territoriale e geografica), dal numero di interessati coinvolti – come numero specifico o come percentuale della popolazione interessata – dalla situazione specifica, dagli interessi effettivi del gruppo di interessati, dalla disponibilità di strumenti mezzi alternativi nonché dalla natura e dalla portata della valutazione dei dati. 34. Importanti fattori di bilanciamento possono essere le dimensioni della zona e il numero di interessati sotto sorveglianza. L'uso della videosorveglianza in una zona isolata (ad esempio, per osservare la fauna selvatica o per proteggere infrastrutture critiche come un'antenna radio privata) deve essere valutato in modo diverso rispetto alla videosorveglianza in una zona pedonale o in un centro commerciale.

Ragionevoli aspettative degli interessati: secondo il Considerando 47, l'esistenza di un legittimo interesse richiede un'attenta valutazione. A questo proposito, occorre includere le ragionevoli aspettative dell'interessato al momento e nel contesto del trattamento dei suoi dati personali. Per quanto riguarda la sorveglianza sistematica, il rapporto tra l'interessato e il titolare del

trattamento può variare significativamente e può influenzare L'interpretazione del concetto di aspettativa ragionevole non dovrebbe basarsi soltanto sulle aspettative soggettive in questione. Il criterio decisivo deve essere invece se un soggetto terzo imparziale possa ragionevolmente aspettarsi e concludere di essere oggetto di sorveglianza nella situazione specifica. Gli interessati possono anche aspettarsi di non essere sorvegliati all'interno di aree accessibili al pubblico – soprattutto se tali aree sono solitamente utilizzate per la convalescenza, la rigenerazione e per attività ricreative – nonché nei luoghi in cui le persone trascorrono del tempo e/o interagiscono, come ad esempio zone di seduta, tavoli in ristoranti, parchi, cinema e strutture per il fitness. In questo caso gli interessi o i diritti e le libertà dell'interessato spesso prevarranno sui legittimi interessi del titolare del trattamento.

Necessità allo scopo di eseguire un compito nell'interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento: i dati personali potrebbero essere trattati mediante la videosorveglianza a norma dell'art. 6, paragrafo 1, lettera e), se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

Consenso (art. 6, paragrafo 1, lettera a): Il consenso deve essere prestato liberamente, deve essere specifico, informato e inequivocabile, come descritto nelle linee guida sul consenso. Per quanto riguarda la sorveglianza sistematica, il consenso dell'interessato può fungere da base giuridica ai sensi dell'art. 7 (cfr. il considerando 43) solo in casi eccezionali. È nella natura della sorveglianza il fatto che questa tecnologia consenta di controllare contemporaneamente un numero non noto di persone. Il titolare del trattamento difficilmente sarà in grado di dimostrare che l'interessato ha prestato il consenso prima del trattamento dei suoi dati personali. Supponendo che l'interessato revochi il proprio consenso, sarà difficile per il titolare dimostrare che i dati personali non sono più oggetto di trattamento (art. 7, paragrafo 1).
Nel caso del trattamento dati effettuato tramite i sistemi di videosorveglianza attivati secondo i presupposti richiamati nel presente documento non è richiesto il consenso dell'interessato.

Comunicazione di filmati a terzi: in linea di principio, le norme generali del G.D.P.R. si applicano alla comunicazione di videoregistrazioni a soggetti terzi. La comunicazione è definita all'art. 4, paragrafo 2, come trasmissione (comunicazione individuale), diffusione (pubblicazione online) o qualsiasi altra forma di messa a disposizione. I soggetti terzi sono definiti all'art. 4, paragrafo 10. In caso di comunicazione a paesi terzi o organizzazioni internazionali, si applicano anche le disposizioni speciali dall'articolo 44 e ss. Qualsiasi comunicazione di dati personali costituisce uno specifico trattamento per il quale il titolare deve avere una base giuridica.

Secondo l'art. 6, paragrafo 1, lettera c), il trattamento è lecito se è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento. Sebbene le attività di polizia siano disciplinate in via esclusiva dalle norme vigenti nei singoli Stati membri, è molto probabile che esistano norme generali che disciplinano il trasferimento delle prove alle autorità di contrasto in ogni Stato membro. Il trattamento eseguito dal titolare che consegna i dati è disciplinato dal

G.D.P.R. Se la normativa nazionale impone al titolare del trattamento di cooperare con le autorità di contrasto (per esempio nelle indagini), la base giuridica per la trasmissione dei dati è un obbligo legale di cui all'art. 6, paragrafo 1, lettera c).
Spesso, quindi, il rispetto dei requisiti di limitazione della finalità di cui all'arT. 6, paragrafo 4, non risulta problematico, in quanto la comunicazione è disciplinata esplicitamente dal diritto degli Stati membri. Non è quindi necessario prendere in considerazione i requisiti specifici riferiti all'eventuale cambiamento di finalità ai sensi delle lettere a) -e) dell'art. 6.

Un ulteriore punto di criticità rispetto al trattamento dati personali riconducibile alla sorveglianza su vasta scala di aree pubbliche è rappresentato dalla necessità di rendere disponibile l'informativa, in particolare rispetto alle "modalità operative" da adottare.

L'informativa agli interessati può essere fornita mediante affissione di cartelli informativi nei punti e nelle aree in cui si svolge la videosorveglianza, che contengano anche indicazioni su come e dove reperire un testo completo contenente tutti gli elementi di cui all´art. 13 del Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, come peraltro esplicitato dalla FAQ n. 4) pubblicata sull'argomento dall'Autorità Garante .

L'informativa può essere fornita utilizzando un modello semplificato, che deve contenere, tra le altre informazioni, le indicazioni sul titolare del trattamento e sulla finalità perseguita. Il modello può essere adattato a varie circostanze (presenza di più telecamere, vastità dell'area oggetto di rilevamento o modalità delle riprese). L'informativa va collocata prima di entrare nella zona sorvegliata. Non è necessario rivelare la precisa ubicazione della telecamera, purché non vi siano dubbi su quali zone sono soggette a sorveglianza e sia chiarito in modo inequivocabile il contesto della sorveglianza. L'interessato deve poter capire quale zona sia coperta da una telecamera in modo da evitare la sorveglianza o adeguare il proprio comportamento, ove necessario.

Nel caso di specie, le informative presenti sono state rilevate non conformi e viene data indicazione di verificare l'adozione dei modello idoneo e con posizionamento coerenti con lo stato dei luoghi.

Trattamenti riguardanti categorie particolari di dati: solitamente, i sistemi di videosorveglianza raccolgono enormi quantità di dati personali che possono rivelare dati di natura altamente personale e persino categorie particolari di dati. Infatti, dati apparentemente non significativi, all'origine raccolti tramite video, possono essere utilizzati per ricavare altre informazioni e raggiungere uno scopo diverso da quello iniziale (ad esempio per mappare le abitudini di un individuo). Tuttavia, la videosorveglianza non sempre è considerata un trattamento di categorie particolari di dati personali.
Come specificato dalla Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - Versione 2.0 adottate il 29/01/2020, a titolo esemplificativo, le riprese video che mostrano un interessato che indossa occhiali o utilizza una sedia a rotelle non sono di per sé considerate

categorie particolari di dati personali. Pur tuttavia, si potrebbero, ad esempio, dedurre le opinioni politiche da immagini che mostrano interessati identificabili mentre partecipano a un evento, a uno sciopero, ecc. Questo caso rientrerebbe nell'ambito di applicazione dell'art. 9.

In via generale e in linea di principio, ogniqualvolta si installa un sistema di videosorveglianza si dovrebbe prestare particolare attenzione al principio della minimizzazione dei dati. Pertanto, anche nei casi in cui l'art. 9 del G.D.P.R. non trovi applicazione, il titolare del trattamento dovrebbe sempre cercare di ridurre al minimo il rischio di acquisire filmati che rivelino altri dati sensibili. Se un sistema di videosorveglianza è utilizzato per trattare categorie particolari di dati, il titolare del trattamento deve individuare sia un'eccezione che consenta il trattamento di categorie particolari di dati ai sensi dell'articolo 9 (vale a dire un'esenzione dal divieto generale di trattare categorie particolari di dati) sia una base giuridica ai sensi del richiamato art. 6, quale, a titolo di esempio, il caso di cui all'art. 9, paragrafo 2, lettera c) del G.D.P.R. ("[…] il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica […]») – in teoria e in via del tutto eccezionale – ma il titolare del trattamento dovrebbe giustificarlo come una necessità assoluta per tutelare gli interessi vitali di tale persona e dimostrare che "[…] l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso".

Il sistema di videosorveglianza posto del Comune di Valfenera non è utilizzato per trattare categorie particolari di dati se non in via del tutto incidentale e relativo al mero transito delle persone in area pubblica e neppure acquisisce o elabora dati biometrici degli individui.

Applicazione della Direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giudiziarie (direttiva LED): il trattamento dei dati personali da parte delle autorità competenti a fini 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, rientra nella direttiva (UE) 2016/680.

4. SINTESI ANALISI DEL RISCHIO

Art. 35 lettera a)

Ai sensi dell'art. 35 lettera a) del Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 i trattamenti, effettuati mediante il sistema di videosorveglianza, avranno finalità di solo controllo di sicurezza relativamente alle facoltà attribuite dalla legge che ne è base giuridica. Il trattamento di videosorveglianza corrisponde al legittimo interesse perseguito dal titolare all'ordinata erogazione del servizio pubblico, al quale è preposto per ragioni d'istituto e per legge e per perseguire le finalità proprie.

Art. 35 lettera b) valutazione della proporzionalità in relazione alle finalità

La rilevazione delle immagini avviene nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili e la videosorveglianza sarà effettuata nel rispetto del principio di minimizzazione dei dati e comunque pertinenti e non eccedenti rispetto alle finalità perseguite e in conformità delle dalla Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - Versione 2.0 adottate il 29/01/2020.

Art. 35 lettera c) valutazione dei rischi per i diritti e le libertà degli interessati

La libertà è la dignità delle persone riprese quali interessati è assicurata dalla informativa resa ex art. 13 del G.D.P.R. L'informativa viene fornita utilizzando anche un modello semplificato che contiene, tra le altre informazioni, le indicazioni sul titolare del trattamento e sulla finalità perseguita. L'informativa rinvia a un testo completo contenente tutti gli elementi di cui all´art. 13 del Regolamento UE 2016/679.

Art. 35 lettera d) misure tecniche e organizzative rischi, misure di sicurezza, meccanismi per garantire la protezione dei dati personali (caratteristiche tecniche dei dispositivi)

La valutazione del rischio è stata condotta sotto il profilo dell'incidenza sui dati personali e gli interessi legittimi degli interessati e delle altre persone in questione è stata fatta sulla base delle misure tecniche e organizzative in base alle quali, Per la visualizzazione, la consultazione e l'asportazione delle immagini l'accesso è consentito dal personale autorizzato. Inoltre in ognuno di questi casi l'accesso è possibile solo con credenziali personalizzate e solo a seguito di autorizzazione del Designato.

.

Tempi di conservazione delle immagini di videosorveglianza

L'attuale normativa di videosorveglianza stabilisce la durata della conservazione delle immagini registrate, fissando il limite standard a 24 ore, eventualmente estendibili a 48 h, mentre il temine di 7 gg. è consentito soltanto per finalità di pubblica sicurezza. Al termine dei periodi definiti, tutti i dati (flusso video) sono cancellati automaticamente – con sovrascrittura delle immagine - dallo stesso sistema

4.1. MISURE PREVISTE PER AFFRONTARE I RISCHI

Misure tecniche e organizzative: come indicato all'art, 32, paragrafo 1, del G.D.P.R., non è sufficiente che il trattamento di dati personali durante videosorveglianza sia lecito, in quanto titolari e responsabili del trattamento devono anche garantire l'adeguata sicurezza dei dati in questione. Le misure tecniche e organizzative attuate devono essere proporzionate ai rischi per i diritti e le libertà delle persone fisiche derivanti dai casi di distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso ai dati di videosorveglianza. A norma degli artt. 24 e 25 del G.D.P.R., i titolari del trattamento devono mettere in atto misure tecniche e organizzative anche al fine di salvaguardare tutti i principi di protezione dei dati durante il trattamento e di stabilire i mezzi affinché gli interessati possano esercitare i propri diritti secondo la definizione di cui agli artt. 15-22 del Regolamento. I titolari del trattamento devono adottare una struttura interna e politiche in grado di assicurare l'attuazione di tali misure sia al momento di definire i mezzi di trattamento sia all'atto del trattamento stesso, compresa l'esecuzione di valutazioni d'impatto sulla protezione dei dati ove necessario.

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita: come stabilito dall'art. 25 del Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, i titolari del trattamento devono mettere in atto adeguate misure tecniche e organizzative di protezione dei dati non appena pianificano l'installazione di un sistema di videosorveglianza, prima di iniziare la raccolta e il trattamento di filmati. Questi principi sottolineano la necessità di tecnologie integrate per il miglioramento della protezione, impostazioni predefinite che riducano al minimo il trattamento dei dati e l'adozione degli strumenti necessari ai fini della massima protezione possibile dei dati personali.

I rischi identificati connessi all'impiego del sistema videosorveglianza del Comune di Valfenera sono affrontati secondo un triplice approccio:

- previsionale
- procedurale
- tecnico

L'approccio previsionale rimanda ad una politica complessiva di gestione del sistema orientata al controllo ed alla riduzione del rischio, che parte dall'assunto che i rischi non possono essere eliminati ma si possono ridurre al di sotto di una soglia definita "di rischio accettabile". Le strategie possibili per una concreta mitigazione del rischio sono:

- la riduzione della pericolosità viene perseguita diminuendo la probabilità che un certo fenomeno si verifichi con una certa intensità in un certo tempo. Si può intervenire sui fattori di innesco del fenomeno, dopo averli riconosciuti e compreso come generano il fenomeno pericoloso, oppure sul fenomeno stesso, per prevenirne la ripetitività;

- la riduzione della vulnerabilità viene effettuata attraverso interventi tecnici finalizzati a diminuire il grado di danno degli elementi esposti al rischio intervenendo direttamente sui singoli elementi (si tratta di un intervento "indiretto", nel senso che si costruisce e si modifica l'impostazione della videosorveglianza sulla base delle esperienze, anche osservazionali, relative all'incidenza del sistema sulla popolazione in termini di "attacco alla privacy" e di miglioramento della "percezione di sicurezza", concretamente anche attraverso attività di divulgazione, educazione al rischio della cittadinanza,monitoraggio...);

- la riduzione dell'esposizione è uno dei fondamentali mezzi di mitigazione del rischio. Essa può essere effettuata secondo due diverse strategie: a) la pianificazione, che prevede la riduzione o la diversa perimetrazione delle aree ritenute di interesse da sottoporre a videosorveglianza e, potenzialmente, a videoanalisi o la limitazione del raggio di azione degli apparati di ripresa della fruizione delle aree soggette a rischio e b) "l'emergenza" che prevede l'intervento immediato a seguito del verificarsi di un fenomeno (possibile violazione segnalata, criticità rilevate dagli operatori, eventuale allertamento della popolazione per inefficacia o invasività della videosorveglianza, accessi e trattamenti illeciti dei dati personali..);

Obiettivo dell'approccio previsionale è la progressiva riduzione del rischio residuo, cioè il margine di rischio rimanente a seguito degli interventi di mitigazione descritti, sino all'ottenimento di un rischio residuo inferiore al livello di rischio accettabile (quest'ultimo determinabile in base al bilanciamento del diritto alla riservatezza con il diritto alla sicurezza in capo ai cittadini).

L'approccio procedurale, invece, si prefigge di ridurre il rischio di trattamento illecito attraverso l'introduzione di meccanismi gestionali idonei a garantire la protezione dei dati personali acquisiti tramite il sistema videosorveglianza del Comune di Valfenera.

Anche se allo stato non sono stati individuati designati in quanto l'accesso al sistema è riservato (ad oggi) unicamente al titolare del trattamento nella persona del Sindaco pro-tempore, possono essere previste misure di sicurezza focalizzate su eventuali operatori a cui dovessero essere attribuite facoltà o prerogative di accesso che, in parte, costituiscono potenzialmente "l'anello debole" del sistema delle garanzie poste a tutela degli interessati in funzione delle loro concrete possibilità di accesso e intervento sui dati trattati. In particolare, potranno essere adottate procedure atte a impedire eventuali abusi ed a circoscrivere e limitare la possibilità degli operatori di imporre modifiche ai trattamenti di dati personali impostati di default al sistema e precisamente:

- con specifico atto emanato da parte dell'eventuale designato ai singoli incaricati e preposti potranno essere affidati i compiti specifici e prescrizioni puntuali per l'utilizzo dei sistemi;

- prima dell'utilizzo degli impianti, essi dovranno essere istruiti al corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul Regolamento adottato;

- l'eventuale designato autorizza l'accesso, la visualizzazione ed il materiale trattamento solo ad incaricati e preposti di servizi rientranti nei compiti istituzionali dell'Ente e per scopi connessi alle finalità del trattamento;

- l'eventuale designato impartisce idonee istruzioni atte ad evitare assunzioni o rilevamento di dati da parte delle persone autorizzate all'accesso per le operazioni di manutenzione degli impianti;

Inoltre, sempre nell'ambito delle prerogative e competenze del titolare del trattamento nella persona del Sindaco pro-tempore:

- la designazione di eventuali responsabili esterni non dipendenti dell'Ente può essere effettuata solo se l'organismo esterno svolge prestazioni strumentali e subordinate alle scelte del titolare del trattamento;

- gli autorizzati al materiale trattamento dei dati personali gestiscono unicamente quelli ai quali hanno accesso e solo nei limiti in cui essi sono pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso, attenendosi alle istruzioni impartite dal titolare e del responsabile del trattamento;

- nell'ambito degli autorizzati, con l'atto di nomina, i soggetti cui è affidata la custodia e conservazione delle parole chiave e delle chiavi di accesso alla sala di controllo ed alle postazioni per l'estrapolazione delle immagini;

- Il titolare adotta le misure minime di sicurezza per la protezione dei dati personali già a suo tempo indicate dall'art. 34 e dall'Allegato B del Codice in materia di protezione dei dati personali approvato con D.Lgs 196/2003, "disciplinare tecnico in materia di misure minime di sicurezza" e dalle norme concretamente applicabili dettate da AGID. La sicurezza per l'accesso ai dati personali è garantita, in particolare, attraverso:
  - autenticazione informatica;
  - adozione di procedure di gestione delle credenziali di autenticazione;
  - utilizzazione di un sistema di autorizzazione;
  - aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
  - protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti a determinati programmi informatici;

- l'accesso ai sistemi riconducibili all'impianto di videosorveglianza del Comune di Valfenerapotrà essere consentito esclusivamente a soggetti espressamente autorizzati. In presenza di differenti competenze specificatamente attribuite ai singoli operatori dovranno essere configurati diversi livelli di visibilità e trattamento delle immagini e, se tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti dovranno essere in possesso di un profilo di autorizzazione e credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza. In particolare, ciascuno di essi dovrà essere dotato di identificativo e parola chiave, di cui è responsabile per la custodia, la conservazione e la assoluta riservatezza;

- in caso di interventi di manutenzione o di settaggio del sistema, i soggetti abilitati a tali operazioni possono accedere alle immagini solo se strettamente indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;

- l'eventuale spostamento della direzione di ripresa e il cambiamento dei tempi di movimento o delle funzionalità degli strumenti di ripresa è consentito solamente al responsabile, il quale provvede a darne comunicazione scritta agli incaricati e preposti;

- come più volte specificato nel presente documento, l'utilizzo delle telecamere è consentito solo per il controllo di quanto si svolga nei luoghi pubblici mentre non è ammesso nelle proprietà private e, secondo le indicazioni impartite dal titolare e dal designato, gli operatori non possono effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto attivato;

- gli operatori devono rendere utilizzabili i dati disponibili in modo pertinente e non eccedente rispetto alle finalità per le quali è previsto il trattamento, devono trattare i dati disponibili con modalità volte a salvaguardare l'anonimato successivamente alla fase della raccolta, non possono modificare i trattamenti esistenti o introdurre nuovi trattamenti senza esplicita autorizzazione del responsabile, non possono duplicare o creare nuovi archivi o nuove banche dati senza espressa autorizzazione del titolare o dell'eventuale designato, nell'esecuzione dei compiti assegnati, devono attenersi alle regole di ordinaria diligenza al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento e devono mantenere assoluto riserbo sui dati personali di cui vengano a conoscenza nell'esercizio delle proprie funzioni, devono osservare tutte le misure di protezione e sicurezza, già in atto o successivamente disposte, atte ad evitare rischi, anche accidentali, di distruzione, perdita, accesso non autorizzato, o trattamento non consentito o non conforme alle finalità della raccolta dei dati personali;

- fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere esaminati, nel limite del tempo ammesso per la conservazione (7 giorni),

solo in caso di effettiva necessità per il conseguimento delle finalità indicate dal Regolamento adottato;

- l'accesso alla sala di controllo, ubicata presso il palazzo municipale di Valfenera, è consentito unicamente al Sindaco pro-tempore nella sua qualità legale rappresentante dell'Ente (titolare) e/o suoi eventuali delegati e ai soggetti designati/autorizzati con formale provvedimento e/o specifiche anche estemporanee esigenze;

- eventuali accessi di persone diverse da quelle sopra indicate possono essere autorizzati per iscritto Sindaco. Possono essere autorizzati all'accesso solo gli incaricati dei servizi rientranti nei compiti istituzionali dell'Ente di appartenenza e per scopi connessi alle finalità specifiche, nonché il personale addetto alla manutenzione degli impianti ed alla pulizia dei locali, i cui nominativi dovranno essere comunicati per iscritto;

- la mancata osservanza degli obblighi previsti al presente articolo espone i trasgressori l'applicazione di sanzioni disciplinari e, nei casi previsti dalla normativa vigente, del regime sanzionatorio previsto per le diverse fattispecie.

L'approccio tecnico rimanda alla progettazione e pianificazione della sicurezza della rete e dei sistemi informativi/informatici ed essa riconducibili.

L'impianto (rete) riconducibile al sistema videosorveglianza del Comune di Valfenera, assicura la crittografia dei flussi video in accordo a quanto richiesto al paragrafo 3.3.1 comma f) "utilizzo di reti pubbliche e connessioni wireless" del Provvedimento dell'Autorità Garante per la protezione dei dati personali, in materia di videosorveglianza del 08/04/2010 (G.U. n. 99 del 29/04/2010). Le stesse cautele sono adottate per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie wi-fi, wi-max, Gprs). Gli apparati medesimi sono protetti contro i rischi di accesso abusivo di cui all'art. 615-ter C.P.

Le Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - Versione 2.0 adottate il 29/01/2020 riportano esempi concreti di misure pertinenti. La maggior parte delle misure che possono essere utilizzate per la sicurezza dei trattamenti di videosorveglianza, soprattutto quando si utilizzano apparecchiature digitali e software, sono sostanzialmente identiche alle misure utilizzate in altri sistemi informatici. Tuttavia, indipendentemente dalla soluzione prescelta, il titolare del trattamento deve proteggere adeguatamente tutti i componenti di un sistema di videosorveglianza e i dati in tutte le fasi, vale a dire durante la conservazione (dati a riposo), la trasmissione (dati in transito) e il trattamento (dati in uso).

Nel selezionare le soluzioni tecniche, il titolare del trattamento dovrebbe considerare le tecnologie che tutelano la sicurezza dei dati. Esempi di questo tipo di tecnologie sono i sistemi che consentono il mascheramento o l'offuscamento delle zone irrilevanti per la sorveglianza, oppure

l’editing di immagini di terzi, quando si forniscono filmati agli interessati. vasta letteratura, comprese le norme internazionali e le specifiche tecniche sulla sicurezza fisica dei sistemi. Oltre alla eventuale necessità di una valutazione d’impatto sulla protezione dei dati (Data Protection Impact Assessment, DPIA).
Nell’elaborare le proprie politiche e procedure di videosorveglianza i titolari del trattamento dovrebbero prendere in considerazione gli elementi indicati di seguito:

- Responsabilità della gestione e del funzionamento del sistema di videosorveglianza.
- Finalità e ambito di applicazione del progetto di videosorveglianza.
- Utilizzo appropriato e vietato (dove e quando la videosorveglianza è consentita e dove e quando non lo è)
- Misure di trasparenza
- Modalità e durata delle registrazioni video, compresa la conservazione delle videoregistrazioni relative a problemi di sicurezza
- Procedure operative
- Gestione dei problemi e procedure di recupero

Misure tecniche: sicurezza fisica di tutti i componenti del sistema, nonché integrità del sistema, vale a dire protezione e resilienza in caso di interferenze volontarie e involontarie nel suo normale funzionamento e controllo degli accessi. Riservatezza (i dati sono accessibili solo a coloro a cui è concesso l’accesso), integrità (prevenzione della perdita o della manipolazione dei dati) e disponibilità (i dati possono essere consultati ogniqualvolta sia necessario), protezione della trasmissione di filmati attraverso canali di comunicazione sicuri a prova di intercettazione, cifratura dei dati; utilizzo di soluzioni basate su hardware e software quali firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici, rilevamento di guasti di componenti, software e interconnessioni, garanzia che tutti i locali in cui viene effettuato il monitoraggio mediante videosorveglianza e in cui vengono conservate le riprese video siano protetti contro l’accesso non supervisionato da parte di terzi, posizionamento dei monitor in modo tale che solo gli operatori autorizzati possano visualizzarli, definizione e l’applicazione delle procedure per la concessione, la modifica e la revoca dell’accesso, attuazione di metodi e mezzi di autenticazione e autorizzazione dell’utente, tra cui ad esempio la lunghezza delle password e la frequenza della loro modifica.

Accesso degli interessati: gli interessati, cioè i soggetti ripresi, devono poter accedere alle riprese che li riguardano e verificare le modalità di utilizzo dei dati raccolti (esercizio dei diritti).

Il complesso di tali procedure può essere ragionevolmente applicato dal titolare del trattamento, per quanto di competenza e per quanto riconducibile alle proprie strutture operative.

Inoltre, si è proceduto, come da indicazioni dell’Autorità Garante nazionale, ad una valutazione preliminare della DPIA attraverso il software messo a disposizione dalla CNIL (Commission Nationale de l'Informatique et des Libertés - Autorità francese per la protezione dei dati)

denominato PIA (Privacy Impact Assesment) che, pur non costituendo un modello a cui fare riferimento per ogni tipologia di trattamento e che nel caso di specie presenta anomalie rispetto alla terzietà delle valutazioni e validazioni, offre comunque un focus semplificato sugli elementi principali di cui si compone la valutazione di impatto, le cui risultanze di ripropongono qui a seguito:

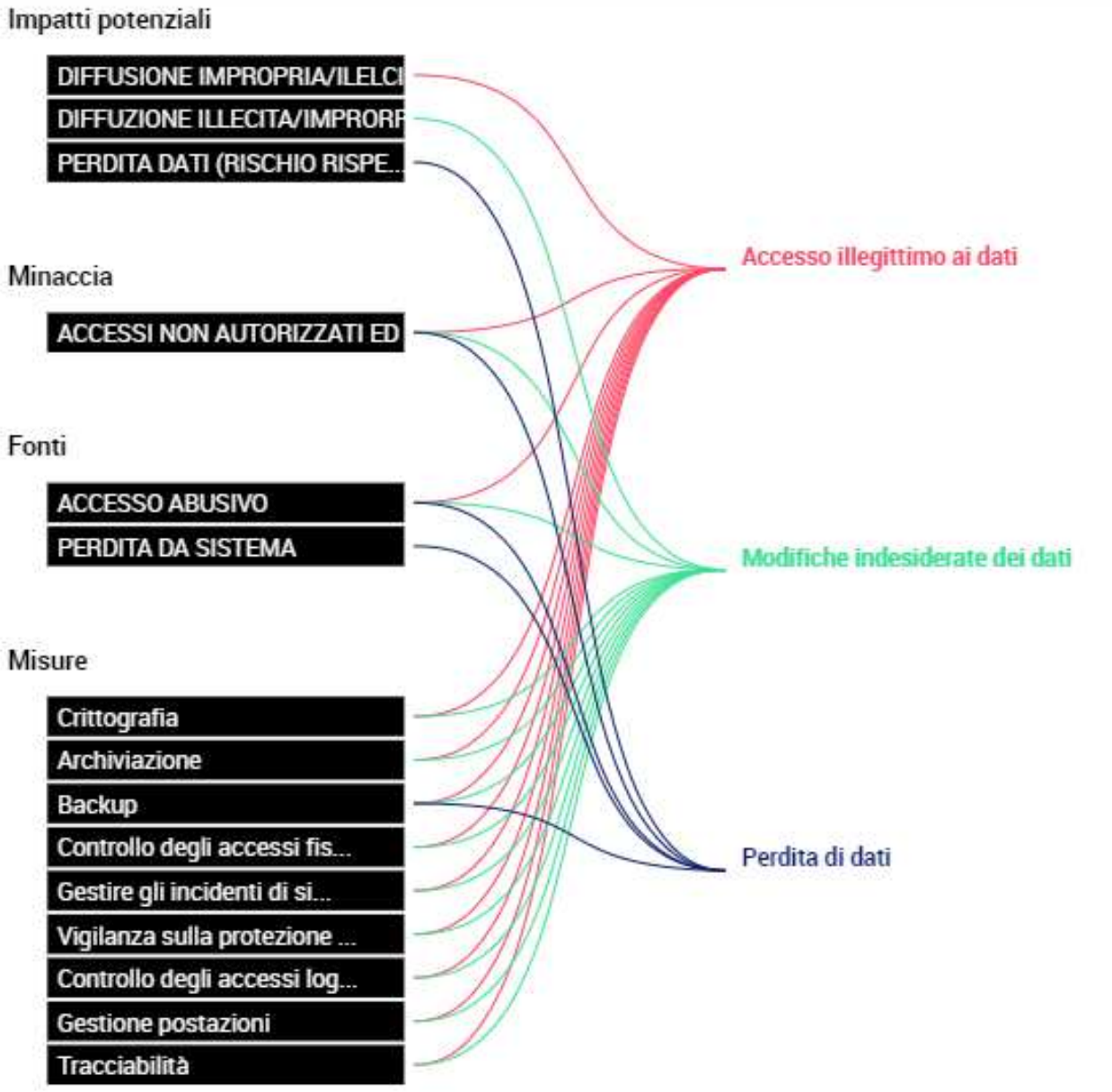

Fig. 19 - CNIL Commission Nationale de l'Informatique et des Libertés – Outil PIA - PANORAMICA DEI RISCHI (panoramica globale e sintetica degli effetti prodotti dalle misure sulle componenti di rischio che esse contribuiscono a mitigare)

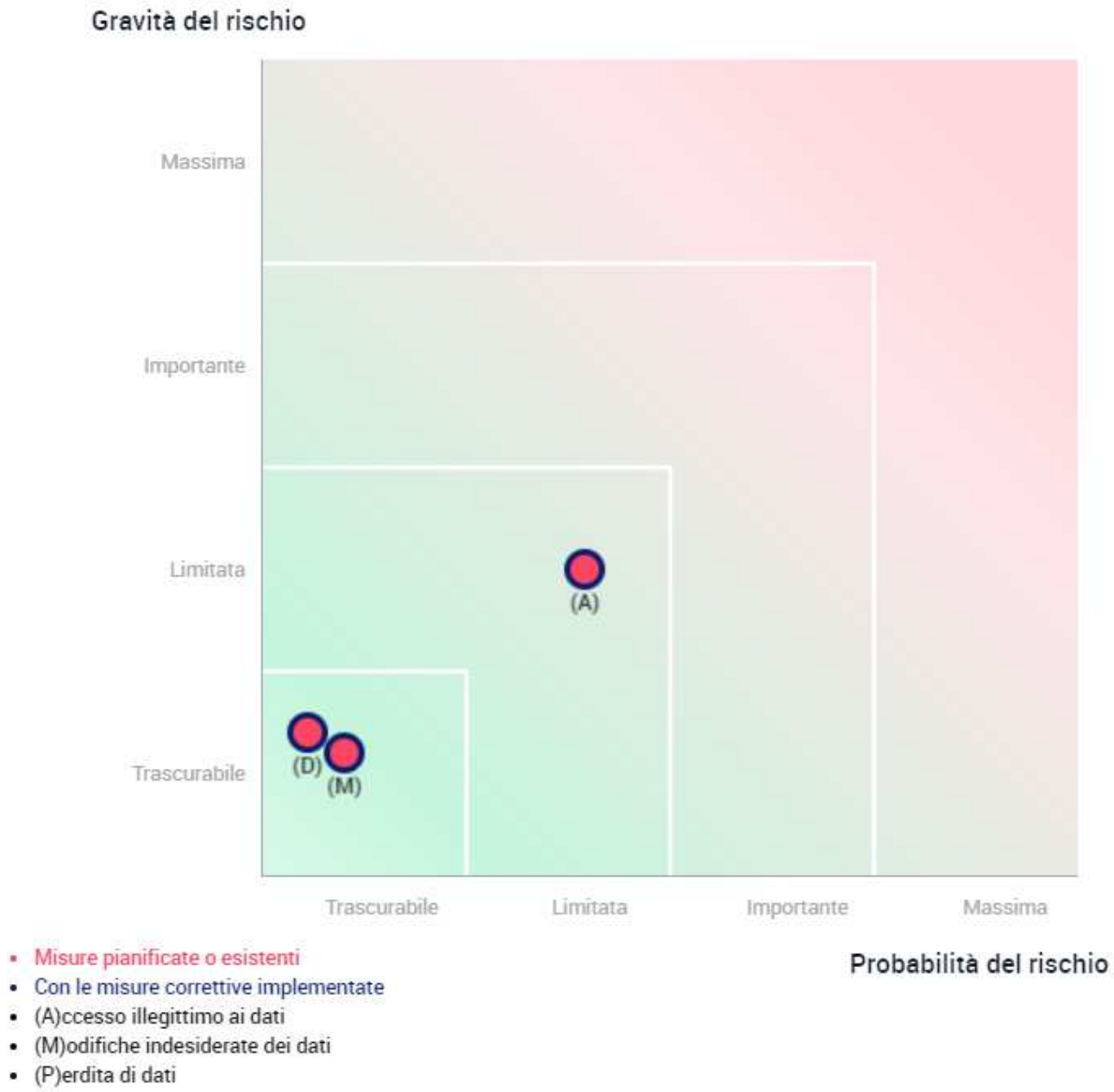

Fig. 20 - CNIL Commission Nationale de l'Informatique et des Libertés – Outil PIA - MAPPATURA DEL RISCHIO (posizionamento del rischio prima e dopo l'applicazione delle misure aggiuntive)

Fig. 21 - CNIL Commission Nationale de l'Informatique et des Libertés Outil PIA – PIANO D'AZIONE (convalida)

5. CONCLUSIONI

Ai sensi del Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, spetta al titolare del trattamento, con il supporto del Responsabile della Protezione dei Dati, condurre una valutazione di impatto sulla protezione dei dati, sulla base dei necessari presupposti normativi, tecnologici, di sicurezza e fattuali e di dare pubblicità per estratto. Il Responsabile della Protezione dei Dati nella presente valutazione d'impatto ha assistito il titolare ed il designato nello svolgimento della valutazione in ossequio al principio di "protezione dei dati fin dalla fase di progettazione" (Data Protection By Design).

La base giuridica della specifica attività (trattamento) è prevista dal D.L. 20/02/2017 n. 14 "Disposizioni urgenti in materia di sicurezza delle città" convertito con modificazioni dalla L. 18/04/2017 n. 48 e che corrisponde all'esercizio di un'attribuzione di pubblico potere al Comune. Sulla base della positiva valutazione d'impatto, sui diritti, libertà e dignità delle persone, si rileva che la finalità della videosorveglianza, per motivi di Pubblica Sicurezza e sicurezza urbana e connesse attività di Polizia Giudiziaria, pone in capo al titolare la predisposizione di misure di sicurezza tecniche ed organizzative adeguate e i relativi trattamenti sono conformi alle previsioni del G.D.P.R., secondo il livello di rischio rilevato, contemperando le esigenze di tutela della scurezza generale dei cittadino con quelle della riservatezza, in modo particolare rispetto ai tempi di conservazione dei dati personali ed alla dislocazione dei sistemi di ripresa .

Le misure tecniche ed organizzative adottate, in relazione all'art. 30, paragrafo 1, del G.D.P.R. sono da ritenersi idonee e commisurate ad un rischio basso\medio per i diritti e le libertà di persone fisiche. Il periodo massimo di conservazione allo stato attuale, in relazione all'atto di adozione del presente documento di valutazione di impatto è stato portato alla conservazione massima di 7 giorni e perciò non risulta necessari alcuna istanza all'Autorità Garante.

Sulla base di quanto illustrato ed argomentato a seguito delle indicazioni scaturite anche dalla verifica preliminare a suo tempo condotta, si ritiene che il trattamento di dati personali riconducibile all'esercizio del sistema di videosorveglianza del Comune di Valfenera rispetti i principi di liceità, necessità, proporzionalità e finalità e sia aderente alle disposizioni di cui al Regolamento Generale sulla Protezione dei Dati (G.D.P.R.) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016, oltre che inquadrabile in termini generali nel dettato delle Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - Versione 2.0 adottate il 29/01/2020. Si esclude, di conseguenza, la presenza di un rischio elevato associato a carenza di misure di protezione che possano giustificare il ricorso ad una pronuncia dell'Autorità Garante.

Si segnala, tuttavia, la necessità di valutare, da parte del titolare, alcuni elementi specifici:

- definire compiutamente il necessario "organigramma privacy" con particolare riferimento alle designazioni/autorizzazioni all'accesso ai dati e le conseguenti iscrizioni al registro dei trattamenti;
- introdurre procedure funzionali a codificare la gestione delle richieste di esercizio dei diritti dell'interessato ai sensi degli artt. 12 e ss. Del G.D.P.R. ed alle richieste di accesso ai dati (immagini) da parte di soggetti istituzionali o aventi diritto;
- verificare l'aggiornamento della cartellonistica e delle informative di primo e secondo livello;
- **motivare compiutamente i presupposti sottesi alla specifica politica di controllo del territorio, che consente all'Amministrazione l'utilizzo degli impianti comunali di videosorveglianza ai fini di prevenzione e repressione di atti delittuosi in aderenza a quanto previsto dal D.M. Interno del 05/08/2008 e dalla L. 18/04/2017, n. 48 (conversione in legge del D.L 20/02/2017, n. 14 recante disposizioni urgenti in materia di sicurezza delle Città) che definiscono e circoscrivono gli ambiti di applicazione della "incolumità pubblica e della sicurezza urbana" ed i conseguenti interventi del Sindaco, in riferimento alla prevista implementazione del sistema di videosorveglianza esistente**.
- valutare se, a seguito di specifica implementazione, il sistema videosorveglianza del Comune di Valfenera consenta tecnicamente l'applicazione della cd "privacy mask" che, in situazioni particolari ed in presenza di un rischio concreto, potrà essere configurata per l'area di ripresa di una singola telecamera;
- indicare specificamente che il sistema di videosorveglianza comunale non può essere utilizzato per il rilievo delle infrazioni al C.d.S. ma per il solo monitoraggio dei flussi di traffico o di eventuali situazioni di pericolo per la viabilità;
- procedere all'aggiornamento del Regolamento per la gestione dei dati personali acquisiti mediante il sistema di videosorveglianza
- procedere alla regolamentazione dell'eventuale condivisione dell'accesso all'impianto di videosorveglianza con le forze di Polizia dello Stato, definendo (come livello minimo) un disciplinare che regoli ruoli, responsabilità e finalità dell'accordo di collaborazione esaltando la trasparenza funzionale dell'organizzazione a tutela del corretto trattamento dei dati e dei diritti fondamentali delle persone fisiche, fissando anche obiettivi strategici dell'impianto oppure (livello ottimale) addivenire ad una contitolarità del trattamento o ad una titolarità autonoma in base alla concreta possibilità tecniche di interconnessione garantite dall'infrastruttura hardware e software.

Il TITOLARE DEL TRATTAMENTO

Visto
Il Responsabile della Protezione dei Dati