CITTA' DI TORINO

REGOLAMENTO

PER LA

DISCIPLINA DELLA

VIDEOSORVEGLIANZA

SUL TERRITORIO DEL

COMUNE DI TORINO

Approvato con deliberazione del Consiglio Comunale n.806 del 2024

INDICE

CAPO I
DISPOSIZIONI GENERALI

Art. 1 – Oggetto
Art. 2 – Finalità e base giuridica
Art. 3 – Definizioni
Art. 4 – Principi applicabili al trattamento dei dati personali

CAPO II
SOGGETTI

Art. 5 – Titolare
Art. 6 – Designato
Art. 7 – Incaricati
Art. 8 – Soggetti esterni

CAPO III
TRATTAMENTO DEI DATI PERSONALI

Art. 9 – Modalità di raccolta dei dati
Art. 10 – Conservazione
Art. 11 – Misure di sicurezza
Art. 12 – Diritti degli interessati
Art. 13 – Violazione dei dati personali

CAPO IV
DISPOSIZIONI SPECIFICHE

Art. 14 – Sistema integrato Pubblico/Privato
Art. 15 – Forme di partecipazione interistituzionale
Art. 16 – Implementazione del sistema con forme di A.I.

CAPO V
TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Art. 17 – Reclamo al Garante e ricorso all'Autorità giudiziaria

CAPO VI
DISPOSIZIONI FINALI

Art. 18 – Entrata in vigore
Art. 19 – Norma di rinvio

CAPO I
DISPOSIZIONI GENERALI

Art. 1
Oggetto

1. Il Comune di Torino utilizza sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico o di propria esclusiva pertinenza ai fini di:
   - tutela della sicurezza urbana, ai sensi del comma 7 dell'art. 6 del Decreto Legge 23 febbraio 2009 n. 11 convertito, con modificazioni, nella legge 23 aprile 2009, n. 38;
   - prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria, in attuazione dei "Patti per la Sicurezza Urbana" sottoscritti dalla Città, ai sensi dell'art. 5, comma 2, lett. a) del Decreto legge 20 febbraio 2017, n. 14, convertito, con modificazioni, nella Legge 18 aprile 2017, n. 48;
   - rilevazione e controllo del traffico;
   - tutela della proprietà e prevenzione degli atti di vandalismo o danneggiamento degli immobili comunali e dei beni facenti parte del patrimonio comunale;
   - sorveglianza, controllo e sicurezza di spazi e ambienti di esclusiva pertinenza comunale;
   - specifiche esigenze di sicurezza del lavoro.
2. 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, le Province autonome di Trento e di Bolzano e gli enti locali, nel rispetto delle rispettive competenze e funzioni.
3. Il presente Regolamento disciplina le modalità di raccolta, trattamento e conservazione dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al comma 1 attivati nel territorio comunale e gestiti dal Comune di Torino, per le finalità sopra indicate.
4. Con il presente Regolamento si garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.
5. In particolare, il presente Regolamento:
   a) definisce le modalità di utilizzo degli impianti di videosorveglianza;
   b) disciplina gli adempimenti, le garanzie e le tutele per il legittimo e pertinente trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza.

Art. 2
Finalità e base giuridica

1. Il trattamento dei dati acquisiti per mezzo dei sistemi di videosorveglianza gestiti dal Comune di Torino è lecito essendo 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.

2. In attuazione del principio di limitazione delle finalità ex art. 5 lett. b) Regolamento (UE) 2016/679, secondo cui il titolare del trattamento è tenuto a definire gli scopi in base ai quali ha intenzione di raccogliere e trattare i dati, i sistemi di videosorveglianza cittadini sono utilizzati per lo svolgimento delle funzioni riconducibili ai seguenti ambiti generali:
    a) garantire la protezione e l'incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati svolti dai soggetti pubblici, alla razionalizzazione e miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti, nel quadro delle competenze attribuite ai Comuni dalla legge;
    b) documentare la violazione delle disposizioni in materia di circolazione stradale;
    c) tutela della proprietà e prevenzione degli atti di vandalismo o danneggiamento degli immobili comunali e dei beni facenti parte del patrimonio comunale;
    d) sorveglianza, controllo e sicurezza di spazi e ambienti di esclusiva pertinenza comunale;
    e) controllo del deposito dei rifiuti volto ad accertare sia l'utilizzo abusivo di aree pubbliche impiegate come discariche di rifiuti ed altri materiali che possono nuocere alla salute dei cittadini, sia l'utilizzo delle aree destinate al conferimenti dei rifiuti in violazione delle norme del Regolamento comunale in materia di gestione dei rifiuti urbani;
    f) consentire l'acquisizione di prove nell'ambito di indagini di polizia giudiziaria;
    g) specifiche esigenze di sicurezza del lavoro connesse alla tutela dell'incolumità degli operatori in specifiche situazioni di pericolo che giustificano l'attivazione di telecamere mobili.
3. Il sistema di videosorveglianza cittadino comporta esclusivamente il trattamento di dati personali che riguardano i soggetti in transito nell'area sottoposta a videosorveglianza.

Art. 3
Definizioni

1. Ai fini del presente Regolamento si intende:
    a) per "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;
    b) per "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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
    c) per "interessato" la persona fisica identificata o identificabile di cui alla lettera b) del presente Regolamento cui si riferisce uno o più dati personali;
    d) per "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. In questa accezione il titolare del

trattamento è il Comune di Torino, rappresentato dal Sindaco pro tempore o da suo delegato, cui competono le decisioni in ordine alle finalità ed ai mezzi del trattamento dei dati personali; il Titolare del trattamento esercita le proprie prerogative, poteri e doveri attraverso i Designati di cui all'art. 4 del Regolamento comunale n. 387/2019 secondo le competenze, prerogative e responsabilità specificate per iscritto nell'atto di designazione;

e) per "Responsabile del trattamento" la persona fisica o giuridica che effettua un trattamento per conto del Titolare;
f) per "Responsabile della protezione dei dati" la persona designata dal Titolare con funzioni, tra le altre, di consulenza, informazione e sorveglianza circa l'osservanza al Regolamento (UE) 2016/679 delle politiche del Titolare del trattamento in materia di protezione dei dati personali;
g) per "incaricati o persone autorizzate al trattamento" le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Designato;
h) per "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;
i) per "Garante per la protezione dei dati personali" l'Autorità di controllo indipendente nazionale incaricata, tra l'altro, di controllare l'applicazione del Regolamento (UE) 2016/679 e della normativa nazionale al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento, e di agevolare la libera circolazione dei dati personali all'interno dell'Unione;
j) per "comunicazione" il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'art. 2-quaterdecies del D. Lgs. 2003/196, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
k) per "diffusione" il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
l) per "dato anonimo" il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non possa essere associato ad un interessato identificato o identificabile;
m) per "limitazione del trattamento" il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
n) per "violazione dei dati personali" la violazione di sicurezza, anche detta "data breach", che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali detenuti, trasmessi, conservati o comunque trattati.

Art. 4
Principi applicabili al trattamento dei dati personali

1. Con il presente Regolamento il Comune di Torino intende garantire che il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche.
2. Tutti i soggetti incaricati delle operazioni connesse all'utilizzo degli impianti di videosorveglianza sono tenuti a garantire che il trattamento dei dati personali si svolga nel

rispetto dei principi di cui al paragrafo 1 dell'art. 5 del Regolamento (UE) 2016/679 e, per quanto di competenza, del paragrafo 1 dell'art. 3 del D. Lgs. 2018/51.

3. In particolare i dati personali acquisiti per mezzo dei sistemi di videosorveglianza saranno:
    a) trattati in modo lecito (ossia per l'esecuzione di un compito di interesse pubblico) corretto e trasparente (apposizione di cartelli ed informativa da fornire agli interessati);
    b) raccolti per finalità determinate (ossia per lo svolgimento delle funzioni istituzionali) esplicite e legittime;
    c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono raccolti, evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti;
    d) esatti e, se necessario, aggiornati, con l'adozione di tutte le misure ragionevoli per cancellare e rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
    e) conservati 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 e protezione dei dati personali mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale;
4. Nel caso di sistemi ubicati in posti di lavoro, il trattamento dovrà avvenire nel rispetto delle disposizioni di cui all'art. 4 della legge 300 del 20 maggio 1970 (statuto dei lavoratori).

CAPO II
SOGGETTI

Art. 5
Titolare

1. Il Comune di Torino, rappresentato ai fini previsti dal Regolamento (UE) 2016/679 dal Sindaco pro-tempore, è il Titolare del trattamento dei dati personali, raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Sindaco può designare per specifici compiti e funzioni i/le Dirigenti dell'ente con specifico provvedimento.
2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dalla normativa europea: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al Regolamento (UE) 2016/679. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dalla normativa europea, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
4. Il Titolare adotta misure appropriate per fornire all'interessato/a:
a) le informazioni indicate dall'articolo 13 Regolamento (UE) 2016/679, qualora i dati personali siano raccolti presso lo/la stesso/a interessato/a;
b) le informazioni indicate dall'articolo 14 Regolamento (UE) 2016/679, qualora i dati personali non siano stati ottenuti presso lo/la stesso/a interessato/a.

5. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi della normativa europea, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo articolo 9.
6. Il Titolare inoltre:
a) designa per specifici compiti e funzioni i/le dirigenti preposti/e alle strutture in cui si articola l'organizzazione comunale;
b) nomina il/la Responsabile della protezione dei dati.

Art. 6
Designato

1. Ai/alle Dirigenti possono essere attribuiti specifici compiti e funzioni connessi al trattamento dei dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. I/le designati/e garantiscono adeguata conoscenza specialistica.
2. Il/la Designato/a provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidati dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare:
- alla predisposizione del Registro dei trattamenti;
- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- ad individuare, contrattualizzare e nominare i/le responsabili di trattamento esterni, nel rispetto delle procedure di cui alla normativa europea;
- a definire le informative per gli/le interessati/e che dovranno essere realizzate ed apposte prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti.
- a svolgere, per la parte di competenza, la valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del Regolamento (UE) 2016/679 nei casi ove essa è obbligatoria o comunque significativa in ordine alla corretta gestione dei trattamenti, anche dopo avere consultato il/la Responsabile Protezione dati;
- a svolgere l'attività preliminare a seguito di ipotesi di perdita di dati (data breach) di cui viene a conoscenza, informandone anche il gruppo di crisi "data breach" se già operativo, ed inoltrare eventuale notifica al Garante, sentito, ove il caso, anche il/la Responsabile Protezione dati; di dette violazioni dovrà darsi conto in un apposito "registro delle violazioni".
3. I/le dipendenti del Comune, sono autorizzati/e dal Designato/a competente al trattamento dei dati riferiti alla struttura di riferimento come individuati/e nel rispettivo registro dei trattamenti. Ai/alle dipendenti autorizzati/e verranno fornite specifiche istruzioni.

Art. 7
Incaricati

1. Il titolare e/o il designato sono tenuti a provvedere alla nomina degli incaricati al trattamento dei dati personali. La nomina è effettuata con atto scritto nel quale sono analiticamente specificati i compiti affidati agli incaricati e le prescrizioni per il corretto, lecito, pertinente e sicuro trattamento dei dati.
2. Gli incaricati sono a tal fine tenuti ad effettuare il trattamento attenendosi scrupolosamente alle istruzioni loro impartite dal titolare e/o designato, nonché alle disposizioni di cui al presente Regolamento.

Art. 8
Soggetti esterni

1. Ai soggetti esterni al Comune di Torino dei quali questo si avvalga, a qualsiasi titolo, per lo svolgimento di servizi ed attività che comportano il trattamento di dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento, si applicano le disposizioni di cui all'art. 28 del Regolamento (UE) 2016/679. I rapporti col titolare saranno disciplinati da un contratto o da un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che stipuli la materia disciplinata ai sensi del comma 3 art. 28 Regolamento (UE) 2016/679.

CAPO III
TRATTAMENTO DEI DATI PERSONALI

Art. 9
Modalità di raccolta dei dati

1. L'attività di videosorveglianza comporta esclusivamente il trattamento dei dati personali rilevati mediante le riprese video e che, in relazione ai luoghi di installazione delle videocamere, interessano i soggetti ed i mezzi di trasporto che transitano nell'area interessata dal raggio d'azione delle videocamere.
2. I dati personali oggetto di trattamento sono:
    a) trattati in modo lecito e secondo correttezza;
    b) raccolti e, laddove previsto, registrati per le finalità di cui all'art. 2 del presente Regolamento;
    c) trattati in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti;
3. In particolare, non vengono effettuate riprese di dettaglio dei tratti somatici delle persone fisiche che non siano strettamente funzionali alle finalità istituzionali dell'impianto attivato. I segnali video delle unità di ripresa sono inviati ai data-center presso le sedi comunali o dei soggetti esterni ex art. 28 Regolamento (UE) 2016/679, dove vengono registrati su appositi

server. L'impiego del sistema di videoregistrazione è necessario per ricostruire l'evento, ai soli fini del soddisfacimento delle finalità di cui all'art. 3 del presente Regolamento.

Art. 10
Conservazione

1. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso dei sistemi di videosorveglianza è limitata al tempo necessario al conseguimento delle finalità per le quali sono acquisite.
2. In base al principio di responsabilizzazione (art. 5, paragrafo 2, del Regolamento europeo) spetta al titolare del trattamento individuare i tempi di conservazione delle immagini, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.
3. I tempi di conservazione relativi a ciascun trattamento sono recepiti nel registro dei trattamenti della Città di Torino.

Art. 11
Misure di sicurezza

1. I dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento sono protetti da misure di sicurezza tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.
2. La sicurezza del dato, intesa a titolo di disponibilità, integrità, riservatezza e protezione dello stesso, viene assicurata dall'implementazione di adeguate misure di Cyber Security previste dal Piano Triennale (ICT) per aumentare il livello di sicurezza e resilienza del sistema informativo della Città.
3. Le misure di sicurezza, tecniche ed organizzative, in particolare dovranno quantomeno assicurare:
    a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori dovranno essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti dovranno essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;
    b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, dovrà essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o di duplicazione;
    c) per quanto riguarda il periodo di conservazione delle immagini, dovranno essere predisposte misure tecniche per la cancellazione, in forma automatica, delle registrazioni, allo scadere del termine previsto;
    d) nel caso di interventi derivanti da esigenze di manutenzione si renderà necessario adottare specifiche cautele quale l'accesso alle immagini, da parte dei soggetti

incaricati a procedere a dette operazioni, solo e ciò si renda effettivamente indispensabile, ed in presenza dei soggetti dotati di credenziali di autenticazione;

e) nel caso si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi dovranno essere protetti contro i rischi di accesso abusivo;
f) la trasmissione tramite una rete pubblica di immagini riprese da apparati di videosorveglianza dovrà essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele andranno adottate per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless.

4. Il titolare e/o il designato assicurano la periodica verifica dell'efficacia delle misure di sicurezza di cui al punto precedente. Inoltre vigilano sulla condotta tenuta da chiunque agisca sotto la loro Autorità e abbia accesso ai dati personali; provvedono altresì ad istruire il personale incaricato sulle finalità e sulle modalità del trattamento, ed in generale su tutti gli aspetti che incidano sui diritti dei soggetti interessati.
5. Nel caso di nomina con atto scritto di un Responsabile esterno ai sensi del precedente art. 8, quest'ultimo dovrà provvedere ad individuare, sempre in forma scritta, le persone fisiche autorizzate al trattamento, specificando, per ognuno, i compiti affidati e le prescrizioni per il corretto, lecito, pertinente e sicuro trattamento dei dati.

Art. 12
Diritti degli interessati

1. E' assicurato agli interessati, identificati o identificabili, l'effettivo esercizio dei propri diritti di cui al Capo III del Regolamento (UE) 2016/679, in particolare di conoscere l'esistenza di trattamenti di dati che possono riguardarli, quindi il diritto di accedere a tali dati, di verificarne le finalità, le modalità del trattamento, e di ottenerne l'interruzione nel caso di palese utilizzo illecito del dato.
2. Con precipuo riferimento al diritto di accesso ai dati raccolti mediante un impianto di videosorveglianza, l'interessato dovrà far pervenire apposita istanza, presentata nei modi previsti dalla legge, indirizzata al titolare e/o designato specificando:
    a) dati del richiedente;
    b) indicazione del luogo in cui è stata effettuata la ripresa;
    c) data e fascia oraria in cui è stata effettuata la ripresa, con un'approssimazione oraria massima di trenta minuti;
    d) eventuali dettagli che possono contribuire ad una agevole individuazione dei frame.
3. In ottemperanza al Principio di Trasparenza e ai sensi art. 13 Regolamento (UE) 2016/679 nelle strade, nelle piazze e nei luoghi in cui sono posizionati i dispositivi del sistema di videosorveglianza cittadino è collocata adeguata segnaletica contenente l'informativa di primo livello, fra cui i dati del titolare del trattamento e le finalità perseguite. 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.
4. L'informativa di primo livello deve rinviare ad un testo più completo, contenente tutti gli elementi di cui all'art. 13 del Regolamento (UE) 2016/679 e pubblicato sulla pagina web del Dipartimento che gestisce l'impianto in oggetto.

Art. 13
Violazione dei dati personali

1. Nel caso in cui si verifichi una violazione di sicurezza che comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali acquisiti, conservati, o comunque trattati a seguito dell'utilizzo del sistema di videosorveglianza comunale, trovano applicazione le disposizioni di cui all'art. 12 del Regolamento comunale n. 387 approvato il 10 giugno 2019, esecutivo dal 24 giugno 2019.

CAPO IV
DISPOSIZIONI SPECIFICHE

Art. 14

Sistema integrato Pubblico/Privato

1. Privati e/o soggetti terzi, singoli o associati, al fine di promuovere la sicurezza integrata sul territorio, possono partecipare all'estensione ed all'implementazione del Sistema di Videosorveglianza di sicurezza urbana mediante l'acquisto diretto ed autonomo di componenti tecnologiche funzionali al monitoraggio del territorio.
2. A tal fine, i soggetti privati devono presentare istanza di partecipazione all'impianto di videosorveglianza comunale, con proprie reti di telecamere riprendenti aree pubbliche, nel rispetto dei principi di cui al presente Regolamento, secondo le condizioni definite dalla Legge n. 48 del 18 aprile 2017, che ha convertito il decreto legge n. 14 del 20 febbraio 2017 recante "Disposizioni urgenti in materia di sicurezza delle città".
3. L'amministrazione comunale valuterà l'idoneità del progetto allegato all'istanza secondo i seguenti criteri:
    a) caratteristiche del sito dal punto di vista della sicurezza urbana;
    b) rispondenza dei dispositivi che si intendono impiegare alle caratteristiche indicate dalla legge;
    c) ottimizzazione dei punti di ripresa;
    d) disponibilità di una linea di telecomunicazione adatta a trasmettere i dati alla rete comunale;
    e) misure di sicurezza adeguate ed allineate a quelle adottate dagli impianti comunali.
4. Se il progetto risulta idoneo, la partecipazione del soggetto privato viene formalizzata in apposita convenzione approvata dalla Giunta Comunale, senza oneri economici a carico dell'Ente.
5. Tali impianti, una volta approvati e realizzati, saranno utilizzati e gestiti esclusivamente dal Comune di Torino.
6. In particolare, le componenti acquistate dai soggetti privati vengono concesse in comodato d'uso al Comune di Torino, che le utilizza in via esclusiva per la gestione di controllo e monitoraggio del territorio e gestione della sicurezza urbana secondo i principi contenuti nel presente Regolamento.
7. I soggetti privati devono garantire, a proprie spese, il corretto funzionamento dell'impianto in termini di manutenzione, assistenza tecnica ed alimentazione elettrica. Non possono

altresì apportare alcuna modifica al sistema senza avere preventivamente ottenuto l'autorizzazione da parte del Comune.

8. Al termine del periodo di validità della convenzione sarà facoltà, previo accordo fra le parti, rinnovare la convenzione alle condizioni stabilite dall'Amministrazione Comunale. In caso contrario sarà compito del privato smantellare l'impianto senza onere alcuno per l'amministrazione comunale, o riconvertirlo per uso esclusivo di protezione della proprietà.

Art. 15
Forme di partecipazione interistituzionale

1. Al fine di perseguire una sempre maggiore sicurezza urbana, attraverso l'implementazione delle misure di controllo del territorio, fra cui i sistemi di videosorveglianza, la Città di Torino si rende disponibile a forme di partecipazione interistituzionale con altri Enti e Forze dell'Ordine.
2. Tale forme di collaborazione andranno individuate e realizzate nell'ambito dei Patti per l'attuazione della sicurezza urbana, e si concretizzeranno in forme avanzate di controllo del territorio, anche attraverso l'implementazione dei sistemi di videosorveglianza già predisposti, così da consentire alle Forze di Polizia la massima condivisione del patrimonio di conoscenza disponibile.

Art. 16
Implementazione del sistema con forme di A.I.

1. Nel rispetto delle indicazioni fornite dall'Autorità garante e dei principi generali in materia di protezione dei dati personali, al fine di ottenere un sistema attivo di analisi, il sistema di videosorveglianza cittadino può essere implementato con specifici algoritmi di intelligenza artificiale che, elaborando le immagini in chiave predittiva, permettono di individuare specifiche criticità in tempo reale incrementando la tempestività di reazione alle emergenze.
2. Nel caso di implementazione dei sistemi tradizionali con algoritmi di Intelligenza Artificiale (A.I.) occorrerà considerare la protezione dei dati fin dalle prime fasi di progettazione. In particolare, poiché l'implementazione potrebbe comportare rischi significativi per i diritti e le libertà delle persone, sarà necessaria una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) che consente di identificare e valutare i rischi associati al trattamento dei dati personali e a sviluppare un piano idoneo per mitigarli.
3. La DPIA dovrà essere adeguata alle specifiche fasi di sviluppo e implementazione del sistema A.I. e prendere in considerazione i rischi specifici associati all'A.I. come l'uso improprio dei dati, la discriminazione automatizzata, la creazione di contenuti falsi, la perdita di controllo sui dati, gli attacchi specifici ai sistemi A.I. e le questioni di confidenzialità.
4. In considerazione della necessità di mantenere un continuo e costante adeguamento ai regolamenti europei e nazionali sull'AI e di tenere conto di altre tipologie di impatti che tali tecnologie potrebbero avere su cittadine e cittadini, per le eventuali modifiche o integrazioni al presente Regolamento si richiederà un parere consultivo al "Board sull'uso etico delle Tecnologie Emergenti per l'innovazione urbana" che opera a titolo consultivo per la Città di Torino, approvato con la deliberazione della Giunta Comunale n. 671, approvata il 31/10/2023, al fine di rendere coerenti le progettualità della Città in tema di innovazione.

CAPO V
TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Art. 17
Reclamo al Garante e ricorso all'Autorità giudiziaria

1. Qualora l'interessato ritenga che i diritti di cui gode in materia di protezione dei dati personali siano stati violati, può proporre reclamo al Garante o ricorso dinanzi all'Autorità giudiziaria.
2. Per tutto quanto attiene al diritto di proporre reclamo all'Autorità Garante si applicano le disposizioni contenute nell'art. 77 del Regolamento (UE) 2016/679 e art. da 140-bis a 143 del Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento.
3. Per tutto quanto attiene al diritto di proporre ricorso all'Autorità giudiziaria si applicano le disposizioni di cui agli art. 78 e 79 del Regolamento (UE) 2016/679 e art. 152 del Codice in materia di protezione dei dati personali.
4. Chiunque subisca un danno, materiale o immateriale, per effetto del trattamento di dati personali ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento ai sensi dell'art. 82 del Regolamento (UE) 2016/679 salvo che questi non dimostrino che l'evento dannoso non gli è in alcun modo imputabile.
5. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi all'Autorità giudiziaria secondo quanto previsto al comma 3 del presente articolo.

CAPO VI
DISPOSIZIONI FINALI

Art. 18
Entrata in vigore

1. Il presente Regolamento entrerà in vigore con il conseguimento della esecutività o della dichiarazione di immediata eseguibilità della deliberazione di approvazione, secondo le leggi vigenti ed osservate le procedure dalle stesse stabilite.

Art. 19
Norma di rinvio

1. Per quanto non espressamente disciplinato dal presente Regolamento si rinvia:
    a) al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;
    b) al Decreto Legislativo 30 giugno 2003, n. 196 così come modificato dal decreto legislativo 10 agosto 2018, n. 101;

c) al Decreto Legislativo 18 maggio 2018, n. 51 relativo al trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali;
d) ai provvedimenti generali sulla videosorveglianza approvati dall'Autorità garante per la protezione dei dati personali;
e) al Regolamento comunale della Città di Torino n. 387 approvato il 10 giugno 2019 ed esecutivo il 24 giugno 2019.