

Rapporto

numero

8282 R

data

27 maggio 2025

competenza

CANCELLERIA DELLO STATO

DIPARTIMENTO DELLE ISTITUZIONI

della Commissione Costituzione e leggi sul messaggio 17 maggio 2025 concernente la Legge sulla videosorveglianza pubblica

1. INTRODUZIONE

In questo inizio di XXI secolo, ogni Stato del nostro pianeta ha il dovere di interrogarsi sull'uso che vuole fare degli strumenti tecnologici, sempre più potenti e sempre meno costosi, che permettono di sorvegliare la popolazione. È quindi più che opportuno che anche il Canton Ticino discuta e introduca una legge-quadro per disciplinare l'uso dei sistemi di videosorveglianza, che sono al momento i più diffusi e potenti fra questi dispositivi di controllo.

Che il tema non sia soltanto una questione tecnica lo dimostra il fatto che, da ormai più di un secolo, lo sviluppo delle tecnologie per la sorveglianza della popolazione è uno degli argomenti che hanno più impegnato il genere letterario della fantascienza.

Fra le opere che hanno offerto riflessioni, profezie e ammonimenti sul tema vale la pena di ricordare in ordine sparso almeno il romanzo *Noi* dello scrittore sovietico in esilio Evgeny Zamyatin (1924), il racconto *Minority Report* di Philip K. Dick (1956) e il romanzo *Kallocaina* (1940) della scrittrice svedese Karin Boye – oltre ovviamente agli arcinoti *Il Mondo nuovo* di Aldous Huxley (1932), *1984* di George Orwell (1949), e *Fahrenheit 451* di Ray Bradbury (1953).

In tempi a noi più vicini, un libro che ha formulato previsioni molto precise, al punto da alimentare qualche sospetto di preveggenza, è *The Circle* dello scrittore statunitense Dave Eggers (2013). Al centro della vicenda c'è una multinazionale nata come piattaforma *social* e diventata un conglomerato onnipotente, che corona la propria crescita con il lancio di un sistema di micro-camere in grado di riprendere in diretta eventi piccoli e grandi che si svolgono in ogni angolo del Pianeta. La trama culmina con la protagonista che diventa la prima persona «trasparente», la cui vita viene trasmessa in diretta globale – una scelta radicale che viene presentata come innocua e libera ma che ben presto diventa obbligatoria, per esempio per i politici, in base al motto secondo il quale «chi non ha nulla da nascondere non ha nulla da temere», sinistra reminiscenza di ciò che amava sostenere il Ministro della propaganda del Terzo Reich, Joseph Goebbels.

Con questa breve carrellata storica – che tralascia altri esempi memorabili, come il film *The Truman Show* di Peter Weir (1998) – desideriamo attirare l'attenzione sulla rilevanza che è stata accordata, nella cultura popolare e in quella «alta», ai problemi che sorgono nel momento in cui chi esercita il potere dispone di strumenti tecnologici in grado di accrescere massicciamente le sue capacità di sorvegliare la popolazione. Questi racconti, romanzi e film hanno avuto, per gli estensori di questo rapporto, la funzione di promemoria sulla delicatezza dell'esercizio al quale ci stavamo accingendo – e sul margine di

imprevedibilità che va tenuto in debito conto, nel pronunciarsi su una legge che punti a disciplinare uno strumento come la videosorveglianza.

Al di là delle questioni che storicamente hanno animato il dibattito sul tema dei dispositivi di controllo, occorre poi considerare le specificità del periodo storico che stiamo vivendo, in cui è fortissima, negli individui e nella società tutta, la tensione fra due bisogni difficilmente conciliabili – quello di sicurezza e quello di libertà.

Se c'è un argomento che in questi anni mette in piena evidenza la tensione fra questi due poli dell'esistenza – e fra ordine e caos, fra paura e coraggio – quell'argomento è sicuramente la videosorveglianza, con le sue profonde implicazioni per la convivenza fra le persone e per il rapporto fra Stato e cittadinanza.

Come se ciò non bastasse, a complicare ulteriormente il quadro c'è il fatto che la fantascienza della quale abbiamo parlato in apertura si è trasformata da genere letterario a cronaca quotidiana. Perché la fantascienza, in questi anni '20 del nuovo secolo, è la nostra casa.

Proviamo a pensare a quale fosse la nostra idea sull'intelligenza artificiale, prima del mese di novembre del 2022. Per chi non masticava tecnologia, sembrava uno scenario teorico riservato ai futurologi, sicuramente lontano dalla nostra vita quotidiana. Poi, i più avventurosi fra noi hanno iniziato a giocare con una nuova applicazione che era stata messa a disposizione gratis su internet – si chiamava ChatGPT. Nel giro di qualche settimana, è stato evidente che avevamo davanti qualcosa che avrebbe rivoluzionato le nostre vite, e che lo avrebbe fatto molto in fretta.

Il resto di questa storia lo stiamo scrivendo e leggendo in presa diretta. Chi segue le notizie sull'argomento, anche solo distrattamente, sa che non sembrano esserci frontiere a quello che l'intelligenza artificiale è in grado di fare. E siamo solo all'inizio.

Questa premessa serve a spiegare l'approccio che ha ispirati gli estensori di questo rapporto, al di là dell'analisi giuridica, nel riflettere su una legge che regolasse l'uso della videosorveglianza in Ticino. Perché si parla di telecamere, certo, ma anche di ben altro.

Sarebbe di una miopia irresponsabile, se questo Legislativo si fermasse al solo hardware e ignorasse tutto ciò che le telecamere portano con sé – se non tentassimo di ragionare insieme, con lungimiranza, sulle sfide aggiuntive che nei prossimi anni (o nei prossimi mesi!) la videosorveglianza porterà con sé.

Un esempio piuttosto estremo di queste sfide viene dai teatri di guerra del Vicino Oriente, dove le telecamere con tecnologie di riconoscimento facciale sono già impiegate per seguire i movimenti di individui sospetti – e, nel caso in cui siano giudicati pericolosi, per eliminarli. È difficile non provare una certa inquietudine leggendo una notizia del genere, benché la Svizzera non sia in guerra, né rischi di viverla nell'immediato futuro.

Allo stesso modo, anche di fronte alle notizie che arrivano dalla Cina, è forte la tentazione di pensare che certe derive autoritarie non potrebbero mai essere accettate in una democrazia occidentale come la nostra. In fondo, ripetiamo a noi stessi, i milioni di telecamere di sorveglianza installate del regime comunista sono pur sempre l'espressione del potere di una dittatura. Noi siamo «liberi e svizzeri», non lo lasceremo mai succedere!

Pensiamo però a un tema molto meno controverso, e molto più vicino alle discussioni politiche che animano ogni giorno le nostre istituzioni: la gestione dei parcheggi. I nostri Comuni oggi devono inviare controllori umani sulle loro strade, per controllare chi viola le regole e infliggere multe. Si tratta di un meccanismo dispendioso e poco efficace. Ecco

perché alcune Città straniere, come Amsterdam, hanno digitalizzato questa attività. Impiegando speciali veicoli dotati di scansionatori, riescono così a fotografare le targhe dei veicoli e a generare automaticamente multe – riducendo quasi a zero la possibilità che un automobilista possa sfuggire alla sanzione.

Le implicazioni della legge che stiamo discutendo, perciò, non appartengono alla fantascienza. Come la vostra Commissione ha scoperto parlando con l'Incaricato cantonale per la protezione dei dati, certi sviluppi tecnologici non sono così lontani dalla Svizzera e dal Ticino. Molti Comuni ticinesi, infatti, hanno già acquistato tecnologie di riconoscimento facciale e di profilazione dei movimenti. Stanno soltanto aspettando il permesso del Cantone per impiegarle nella sorveglianza del loro territorio.

È ovvio che la nuova Legge cantonale sulla videosorveglianza pubblica darà una risposta giuridica negativa a questa richiesta. Si tratta infatti di una tecnologia sproporzionata rispetto al compito che si prefigge. Il progetto legislativo che vi viene sottoposto con questo rapporto ammette solo la videosorveglianza classica, nelle sue diverse modalità di attuazione (dissuasiva, osservativa e invasiva) e vieta invece le applicazioni integrate di riconoscimento facciale o di movimento.

Ciò non significa, tuttavia, che non vale la pena di interrogarsi sulle traiettorie che l'evoluzione di questi strumenti potrebbe seguire, nel futuro a medio e a lungo termine. Perché un conto è ciò che il Parlamento deciderà nel 2025, e un conto ben diverso sono gli sviluppi che si aprono, ogni volta che una telecamera è fisicamente installata sul territorio – e può acquisire nuove funzioni con un semplice aggiornamento del sistema operativo.

L'impressione è che l'argine giuridico che stiamo ponendo con la nuova legge cantonale abbia una tenuta relativa, tutta da verificare – specialmente di fronte a circostanze estreme.

Lo abbiamo visto bene negli Stati Uniti dopo l'11 settembre, quando restrizioni senza precedenti della libertà furono approvate in tutta fretta e senza sostanziali resistenze. Di fronte a un attentato terroristico sul suolo ticinese, o al rapimento di un bambino, o a un evento di gravità paragonabile, sarebbe veramente difficile resistere – e non sfruttare fino in fondo il potenziale che la tecnologia ci mette a disposizione, per di più senza che ci siano costi apparenti a nostro carico.

Senza divagare ulteriormente, cogliamo l'occasione per esprimere l'auspicio che la discussione politica sulla sorveglianza tecnologica del territorio non si concluda con l'approvazione di questa legge. Non possiamo permetterci di prendere alla leggera questi argomenti.

Occorrerà che rimaniamo vigili, di una vigilanza a lungo termine – perché la storia ci ha dimostrato innumerevoli volte, nell'ultimo secolo e mezzo, che chi ha un approccio ingenuo verso le tecnologie si incammina lungo una strada che può portare la società verso luoghi molto oscuri.

2. LA POSIZIONE DEL CONSIGLIO DI STATO

Il Consiglio di Stato, consapevole delle sfide poste dalla crescente diffusione dei sistemi di videosorveglianza pubblica e del loro impatto sui diritti fondamentali, ha ritenuto necessaria l'elaborazione di una legge quadro che disciplini l'uso di queste tecnologie sul territorio cantonale. Questa iniziativa legislativa nasce dalla volontà di colmare un vuoto

normativo, garantendo un quadro chiaro e coerente, allineato ai principi costituzionali di tutela della libertà personale, proporzionalità e protezione dei dati personali.

La posizione del Consiglio di Stato è chiara: la videosorveglianza deve essere uno strumento a supporto della sicurezza pubblica e dell'ordine, ma il suo utilizzo deve rispettare criteri precisi e garantire un equilibrio tra l'interesse pubblico e la tutela delle libertà individuali. In questo contesto, l'obiettivo primario è creare un sistema che risponda alle esigenze di sicurezza senza degenerare in forme di controllo pervasivo della popolazione.

Le motivazioni alla base della proposta legislativa

Secondo quanto illustrato dal Consiglio di Stato nel messaggio n. 8282, la necessità di regolamentare la videosorveglianza deriva da fattori concreti quali:

- **Aumento delle esigenze di sicurezza:** la videosorveglianza è utilizzata per contrastare fenomeni quali criminalità diffusa, degrado urbano, disturbi della quiete pubblica e problematiche di gestione del traffico.
- **Evoluzione delle tecnologie:** i moderni sistemi di sorveglianza consentono non solo riprese standard, ma anche registrazioni dettagliate ad alta risoluzione, analisi dei comportamenti e riconoscimento di volti e targhe, rendendo imprescindibile una regolamentazione chiara.
- **Etica e diritto:** il Consiglio di Stato sottolinea l'importanza di evitare la creazione di banche dati sproporzionate che potrebbero compromettere la riservatezza delle persone e generare rischi di abuso.

La proposta legislativa è pertanto basata sui seguenti principi fondamentali:

1. **Legalità e trasparenza:** la videosorveglianza deve essere disciplinata da una base legale chiara, accessibile e trasparente per la popolazione.
2. **Proporzionalità:** l'utilizzo dei sistemi deve essere commisurato agli scopi perseguiti, evitando l'adozione di misure invasive laddove siano sufficienti interventi meno incisivi.
3. **Finalità specifica:** i dati raccolti non possono essere utilizzati per scopi diversi da quelli previsti, come la repressione di reati o la gestione del traffico.

Ambiti di applicazione e limiti previsti dalla legge

Il Consiglio di Stato ha definito i contesti in cui la videosorveglianza è ammessa:

- **Videosorveglianza dissuasiva:** installazione di videocamere con l'obiettivo di prevenire reati e garantire un effetto deterrente.
- **Videosorveglianza osservativa:** monitoraggio in tempo reale senza registrazione, ad esempio per la gestione del traffico.
- **Videosorveglianza invasiva:** utilizzo limitato per il controllo degli accessi in specifiche strutture pubbliche.

Sono invece escluse dalla normativa le tecnologie di riconoscimento facciale e di profilazione automatica dei comportamenti, considerate sproporzionate rispetto agli scopi di sicurezza pubblica. Inoltre, il Consiglio di Stato pone particolare attenzione ai rischi connessi all'"entrata in vigore di sistemi interconnessi", che potrebbero portare a un monitoraggio onnipresente, o definito anche "di massa".

Considerazioni etiche e prospettive future

Il Consiglio di Stato invita il Gran Consiglio e la popolazione a mantenere un approccio critico e vigile nei confronti dell'evoluzione delle tecnologie di sorveglianza. Pur riconoscendo la necessità di strumenti efficaci per tutelare la sicurezza, rimarca che ogni misura adottata deve essere proporzionata e rispettosa dei diritti fondamentali.

Questa legge, se approvata, rappresenterà un importante argine normativo per prevenire derive autoritarie e garantire che la videosorveglianza resti un mezzo di supporto, mai un fine in sé. Tuttavia, il Consiglio di Stato sottolinea che la regolamentazione deve essere periodicamente aggiornata per rispondere agli sviluppi tecnologici e sociali, evitando così che un apparato normativo statico diventi inefficace o superato.

In sintesi, il progetto legislativo presentato è frutto di una riflessione approfondita sulle esigenze di sicurezza, sull'uso responsabile delle tecnologie e sulla necessità di tutelare la libertà e la privacy dei cittadini. Il Consiglio di Stato auspica che l'approvazione di questa legge rappresenti un punto di partenza per un monitoraggio continuo e una gestione lungimirante della videosorveglianza pubblica.

3. LAVORI COMMISSIONALI

Approccio Commissionale

La Commissione ha riconosciuto che questa legge non può essere affrontata con una semplice analisi politica, ma richiede una visione più ampia che consideri aspetti giuridici, tecnici ed etici. Per comprendere l'importanza del tema, è utile ricordare che la discussione sulla videosorveglianza si inserisce in un contesto più ampio che riguarda anche l'uso del riconoscimento facciale. Secondo un'inchiesta RSI del 2021 intitolata "L'occhio vede, ma cosa guarda?", diverse organizzazioni, tra cui Amnesty International, hanno evidenziato i rischi legati alla sorveglianza biometrica di massa e la mancanza di una chiara regolamentazione in alcuni contesti.

Il metodo seguito si è basato su quattro principali approfondimenti:

- 1. Studio dell'ETH di Zurigo:** La Commissione ha utilizzato lo studio "Automatisierte Erkennung von Stimme, Sprache und Gesicht" come base per comprendere meglio i limiti e le potenzialità delle tecnologie di sorveglianza, in quanto analizza le sfide tecniche, legali e sociali legate al riconoscimento facciale e altre tecnologie correlate. Si evidenziano vantaggi potenziali, come l'identificazione rapida di sospetti e persone scomparse, ma anche rischi significativi, tra cui errori di identificazione e violazioni dei diritti fondamentali. Questo documento ha quindi evidenziato, tra le altre cose, come i contesti socio-tecnici influiscano sull'efficacia dei sistemi e ha sottolineato i rischi legati alle distorsioni nei dati e alle applicazioni di riconoscimento delle emozioni. Inoltre, sono stati messi in luce i rischi di violazioni della privacy, possibili derive verso un controllo pervasivo e l'uso improprio delle informazioni raccolte, elementi che richiedono un'attenta regolamentazione e monitoraggio. Particolare attenzione è data al principio di proporzionalità e alla necessità di restrizioni geografiche e temporali nell'uso di tali sistemi.
- 2. Domande all'Incaricato della protezione dati per il tramite del Consiglio di Stato e audizione del Cancelliere dello Stato, del consulente giuridico del Consiglio di Stato e dell'Incaricato medesimo:** L'Incaricato cantonale della protezione dei dati (ICPD) è l'autorità responsabile di garantire che le istituzioni pubbliche rispettino le

normative sulla privacy e sulla gestione dei dati personali. La Commissione lo ha interpellato, per il tramite del Consiglio di Stato, per la sua esperienza e ruolo nella tutela dei diritti dei cittadini. L'ICPD ha fornito indicazioni fondamentali sui rischi e sulle opportunità legate alla normativa, e sulla necessità di dotarsi di una legge quadro cantonale.

3. **Analisi comparativa:** la Commissione ha svolto un'attenta analisi comparativa, prendendo in considerazione le prassi svizzere e di Paesi vicini, con l'obiettivo di individuare buone pratiche e di evitare modelli normativi problematici. In particolare, sono state esaminate le sentenze dell'Alta Corte federale, così come le decisioni emesse da tribunali di altri Cantoni che hanno già affrontato casi concreti in materia di videosorveglianza. Sono stati inoltre analizzati provvedimenti rilevanti provenienti dall'Italia, valutando sia le soluzioni adottate sia gli orientamenti delle corti superiori e le relative implicazioni giuridiche. Questo lavoro di confronto ha consentito di rafforzare la proposta legislativa con riferimenti solidi, esempi concreti e soluzioni già sperimentate con successo.
4. **Dialogo con i Comuni:** Il percorso descritto si propone di affrontare la tematica in modo responsabile, mettendo al centro l'obiettivo di garantire un equilibrio tra sicurezza pubblica e rispetto dei diritti fondamentali dei cittadini.

3.1 Studio ETH

Lo studio condotto dall'ETH di Zurigo, redatto da Tobias Mahler et al. e pubblicato nel 2023 con il titolo *"Automatisierte Erkennung von Stimme, Sprache und Gesicht"*, ha analizzato in dettaglio le applicazioni di videosorveglianza e riconoscimento facciale, formulando osservazioni e raccomandazioni approfondite.

- **Affidabilità tecnologica:** lo studio descrive come le tecnologie attuali, pur avanzate, presentino limiti significativi in contesti complessi. Le prestazioni possono variare sensibilmente in base alle condizioni ambientali, come la qualità dell'illuminazione e il comportamento dei soggetti. Viene evidenziata la necessità di ulteriori sviluppi tecnici per migliorare la precisione dei sistemi in situazioni reali.
- **Implicazioni per la privacy:** l'ETH ha sottolineato il rischio che l'uso massivo di sistemi di riconoscimento possa compromettere il diritto alla riservatezza e creare un clima di sorveglianza pervasiva. Le informazioni raccolte potrebbero essere utilizzate per scopi non dichiarati o conservate per periodi non giustificati. Lo studio richiama l'importanza di normative trasparenti che stabiliscano chiaramente limiti temporali e finalità specifiche.
- **Raccomandazioni dettagliate:** oltre a richiamare la necessità di regolamentazioni specifiche, lo studio propone di:
 - Definire criteri precisi e pubblici per l'uso delle tecnologie di riconoscimento facciale.
 - Istituire un sistema di autorizzazioni preventive per i progetti di videosorveglianza.
 - Garantire verifiche periodiche da parte di organi indipendenti per monitorare l'efficacia e il rispetto delle regole.
 - Ridurre al minimo le distorsioni nei dati per evitare discriminazioni, prevedendo test e controlli sulla qualità degli algoritmi.
 - Aumentare la formazione degli operatori per un uso consapevole e proporzionato dei sistemi.

Lo studio sottolinea inoltre l'importanza della partecipazione pubblica e del coinvolgimento di esperti multidisciplinari per valutare costantemente l'evoluzione della tecnologia. Queste raccomandazioni hanno fornito spunti essenziali alla Commissione per una riflessione più ampia.

3.2 Risposte del Consiglio di Stato, per il tramite dell'Incaricato cantonale della protezione dei dati, alle proposte della Commissione, e audizione di quest'ultimo, del Cancelliere dello Stato e del Consulente giuridico del Consiglio di Stato

In data 8 settembre 2023, la Commissione ha trasmesso al Consiglio di Stato una serie di osservazioni e proposte relative al messaggio governativo sulla videosorveglianza. In seguito, nella seduta del 24 ottobre 2023, si è svolta un'audizione con il Cancelliere dello Stato, il Consulente giuridico e l'Incaricato cantonale della protezione dei dati, nel corso della quale è emersa l'importanza di garantire un equilibrio tra sicurezza pubblica e tutela dei diritti fondamentali, sottolineando la necessità di stabilire criteri chiari, proporzionalità e trasparenza nell'uso delle tecnologie di sorveglianza.

A riscontro delle osservazioni scritte della Commissione e delle questioni emerse nel corso dell'audizione, il Consiglio di Stato ha trasmesso — in data 20 dicembre 2023 (RG 6331) — un documento redatto dall'ICPD, intitolato *“Risposte dell'ICPD alle osservazioni della CCL dell'8 settembre 2023”*. Tale documento analizza in profondità i principali aspetti sollevati, segnatamente:

• Campo di applicazione della legge

L'ICPD ha ribadito l'importanza di definire in modo preciso il campo di applicazione della legge per evitare sovrapposizioni normative e per garantire la certezza del diritto. Si è chiarito che la legge sulla videosorveglianza pubblica non si applica ai casi in cui:

- le persone non siano identificabili, come ad esempio con videocamere a bassa risoluzione o dispositivi che mascherano automaticamente i volti.
- la sorveglianza venga attuata a scopi esclusivamente personali (es. telecamere domestiche).
- sistemi di ripresa vengano usati esclusivamente per finalità promozionali o turistiche, garantendo che i soggetti ripresi non siano identificabili.

L'ICPD ha sottolineato come queste esclusioni siano conformi al principio di proporzionalità, evitando che la normativa diventi uno strumento troppo invasivo rispetto alle finalità dichiarate.

• Necessità di una base legale solida

Il Consiglio di Stato, tramite l'ICPD, ha accolto la proposta di rafforzare il quadro normativo per garantire una base legale sufficientemente chiara, come richiesto dalla Costituzione e dal principio di legalità. Questo rafforzamento si traduce in:

- La definizione esplicita dei diritti e delle responsabilità degli enti che implementano sistemi di videosorveglianza.

- Procedure standardizzate per la conservazione, l'accesso e la distruzione dei dati raccolti.
- L'obbligo per gli enti pubblici di predisporre valutazioni d'impatto sulla protezione dei dati per ogni nuovo progetto di videosorveglianza.

- **Proporzionalità e minimizzazione dei dati**

L'ICPD ha evidenziato che il principio di proporzionalità deve rimanere il fulcro dell'applicazione della legge. Le telecamere e i sistemi di riconoscimento devono essere utilizzati esclusivamente nei contesti in cui esiste un interesse pubblico prevalente, come la prevenzione di reati o la protezione della sicurezza collettiva. Tuttavia, è fondamentale che:

- I dati raccolti siano limitati allo stretto necessario per raggiungere le finalità dichiarate.
- La conservazione dei dati segua criteri rigorosi e sia limitata nel tempo, con eliminazione automatica una volta superati i termini.

- **Soluzioni tecniche per ridurre i rischi**

Per ridurre i rischi legati a eventuali abusi o violazioni della privacy, il Consiglio di Stato ha proposto:

- L'adozione di tecnologie avanzate che anonimizzano i dati non necessari o irrilevanti.
- La creazione di un sistema centralizzato per la gestione delle telecamere pubbliche, con accesso controllato e audit periodici per verificare l'aderenza alla normativa

- **Coinvolgimento degli attori locali**

Il Consiglio di Stato ha accolto con favore la proposta di un maggiore coinvolgimento degli enti locali nell'attuazione della normativa. Questo approccio prevede che i comuni e altri enti territoriali siano parte attiva nel processo decisionale e che abbiano accesso a linee guida chiare e supporto tecnico-legale per la gestione dei sistemi di videosorveglianza.

- **Conclusioni**

Il Consiglio di Stato ha sottolineato come le osservazioni della Commissione abbiano contribuito a rafforzare il progetto di legge, rendendolo più equilibrato e conforme ai principi fondamentali della protezione dei dati personali. L'ICPD ha ribadito che la legge rappresenta un passo necessario per regolamentare un fenomeno sempre più diffuso e tecnologicamente avanzato, evitando derive lesive dei diritti fondamentali dei cittadini.

3.3 Analisi comparativa

Come detto la Commissione ha condotto un'analisi giuridica sull'utilizzo della videosorveglianza in spazi pubblici, prendendo in esame la giurisprudenza svizzera e di ordinamenti vicini, nonché le basi legali di altri Cantoni, con l'obiettivo di consolidare la base normativa della proposta di legge e di evitare approcci non conformi ai principi fondamentali dello Stato di diritto. Tale lavoro comparativo ha permesso di rafforzare la

coerenza della norma rispetto al principio di legalità, di proporzionalità e di tutela effettiva dei diritti fondamentali.

• **Principio di legalità e necessità di base legale cantonale**

La sentenza 1C_63/2023 del Tribunale federale rappresenta un punto di riferimento imprescindibile: essa stabilisce che i Comuni, per installare sistemi di videosorveglianza su suolo pubblico, devono basarsi su una base legale cantonale chiara, specifica e conforme al principio di legalità. Nel caso in questione, la Città di Lucerna aveva installato delle telecamere su una piazza pubblica invocando la sicurezza come giustificazione.

Il Tribunale ha tuttavia ribadito che la videosorveglianza di spazi accessibili al pubblico costituisce una grave ingerenza nei diritti fondamentali, in particolare nella libertà personale (art. 10 cpv. 2 Cost.) e nella protezione dei dati personali (art. 13 cpv. 2 Cost.). Di conseguenza, tale misura può essere giustificata solo se:

- fondata su una norma di rango legislativo,
- sufficientemente precisa nel delineare scopo, ambito e modalità della videosorveglianza,
- proporzionata rispetto all'obiettivo perseguito.

La sola esistenza di competenze generiche da parte delle autorità comunali, o il riferimento a regolamenti di polizia, non è sufficiente. Il Tribunale ha sottolineato che la possibilità di identificare individui e il potenziale effetto dissuasivo delle telecamere richiedono un controllo rafforzato della legalità.

• **Durata di conservazione dei dati e principio di proporzionalità temporale**

Il trattamento dei dati personali raccolti attraverso sistemi di videosorveglianza deve rispettare anche il principio della proporzionalità temporale, sancito dalla Legge federale sulla protezione dei dati (LPD). In particolare:

- art. 4 cpv. 2 LPD: i dati devono essere trattati solo per lo scopo dichiarato e cancellati una volta esaurita la finalità;
- art. 6 cpv. 2 e 4 nLPD: impone la cancellazione automatica o l'anonimizzazione dei dati al termine del periodo necessario.

La sentenza TF 133 I 77 del 14 dicembre 2006 (caso San Gallo) ha approfondito i criteri per determinare la durata di conservazione, stabilendo che essa deve essere valutata alla luce di:

- accessibilità delle registrazioni;
- grado di protezione contro abusi e accessi non autorizzati;
- natura e gravità dei rischi prevenuti;
- scopo del trattamento.

Il Tribunale ha ammesso la conservazione per 100 giorni in presenza di gravi interessi pubblici (es. lotta alla criminalità contro le persone), ma solo se accompagnata da:

- misure tecniche per impedire accessi illeciti;
- tracciabilità degli accessi;
- uso limitato ai soggetti autorizzati e per finalità definite.

In assenza di tali garanzie, tale durata è sproporzionata. Questo è quanto ha rilevato anche il Tribunale cantonale di Friburgo, che nella sentenza del 20 agosto 2015 (caso della scarica) ha ritenuto eccessiva la conservazione di 100 giorni per la sola protezione di beni materiali, riducendo tale periodo.

• **Confronto con normative cantonali**

L'analisi comparativa ha evidenziato una diversità di approcci tra i Cantoni, ma anche una convergenza verso la limitazione della conservazione a pochi giorni:

- Ginevra (LIPAD): max 7 giorni, estesi fino a 3 mesi solo in caso di procedimenti penali.
- Vaud (LPrD): 7 giorni ordinari, estensione fino a 100 solo con autorizzazione motivata.
- Neuchâtel (LVid): 7 giorni, prorogabili previa autorizzazione del Consiglio di Stato.
- Friburgo (LVid): 30 giorni ordinari, prorogabili fino a 100 solo in caso di danni.
- Berna (PoIG): distruzione obbligatoria entro 100 giorni, salvo procedimenti aperti.
- Basilea Città (IDG): durata ordinaria di 7 giorni.

Le raccomandazioni dell'Incaricato federale della protezione dei dati rafforzano questa impostazione, sottolineando:

- la necessità di limitare al minimo indispensabile la conservazione,
- l'importanza della cancellazione automatica e documentata,
- l'obbligo di giustificare ogni eccezione con un'adeguata analisi del rischio.

• **Garanzie procedurali e prova videoregistrata**

Nella sentenza 6B_899/2020 del 3 agosto 2021, il Tribunale federale ha chiarito che l'utilizzo di immagini video come unico mezzo probatorio deve rispettare pienamente i diritti procedurali della persona coinvolta. Il caso riguardava un cittadino multato per littering, identificato attraverso immagini registrate da un Comune.

Il TF ha accolto il ricorso, sottolineando che anche per infrazioni minori, come quelle amministrative, occorre garantire:

- il diritto di essere sentiti;
- la possibilità di contestare e confrontarsi con gli elementi probatori;
- la trasparenza dell'acquisizione della prova.

• **Esperienze estere: il caso di Como**

Un esempio rilevante a livello internazionale è il caso del Parco Tokamachi di Como (Italia), dove il Comune aveva installato un sistema di videosorveglianza con riconoscimento facciale. Nel 2020, l'Autorità Garante per la protezione dei dati personali ha avviato un'istruttoria e, con Provvedimento n. 54 del 26 febbraio 2020, ha ordinato la disattivazione della tecnologia.

Il Garante ha motivato la decisione affermando che:

- non esisteva una base legale espressa che autorizzasse il trattamento di dati biometrici da parte della polizia locale;

- la misura era sproporzionata rispetto agli scopi (prevenzione di microcriminalità e degrado urbano);
- era possibile raggiungere gli stessi obiettivi con strumenti meno invasivi, come il presidio fisico del territorio.

L'uso del riconoscimento facciale in luoghi pubblici, ha precisato l'Autorità, deve essere eccezionale e giustificato da esigenze assolutamente specifiche.

• **Conclusione**

Le sentenze e i riferimenti normativi analizzati confermano che la videosorveglianza pubblica richiede un quadro normativo solido, preciso e proporzionato. In particolare:

- la necessità di una base legale cantonale chiara e dettagliata è imprescindibile;
- la durata della conservazione dei dati deve essere limitata e giustificata;
- le tecnologie invasive (come il riconoscimento facciale) devono essere oggetto di regolamentazione specifica e usate solo come extrema ratio;
- il rispetto delle garanzie procedurali è essenziale anche per infrazioni minori.

Questi principi devono essere alla base dell'impostazione adottata nella proposta legislativa in esame.

3.4 Dialogo con i Comuni

Nel corso dei lavori, la Commissione ha voluto conoscere il punto di vista degli enti locali, sia in relazione al messaggio sulla protezione dei dati (oggetto di un separato rapporto), sia a quello sulla videosorveglianza, ascoltando direttamente i rappresentanti dei principali Comuni ticinesi. Durante l'audizione, i rappresentanti delle Città di Bellinzona, Chiasso, Lugano, Locarno e Mendrisio, insieme al Presidente dell'Associazione dei Comuni ticinesi (ACT), Felice Dafond, hanno espresso forti perplessità in merito alla nuova legge cantonale sulla protezione dei dati e ad alcuni aspetti del progetto di legge sulla videosorveglianza.

Le normative in discussione sono state percepite come un'ulteriore limitazione dell'autonomia locale, nonché come un esempio di imposizione dall'alto privo di un adeguato coinvolgimento dei Comuni. Il Presidente dell'ACT ha sottolineato come numerose disposizioni previste dalla legge sulla protezione dei dati risultino sovrapposte alla normativa federale, generando incertezza giuridica e il rischio di ricorsi. In particolare, è stata criticata l'estensione della protezione dei dati anche alle persone giuridiche – elemento non previsto a livello federale – che potrebbe risultare incompatibile con il diritto superiore.

I sindaci hanno inoltre evidenziato come una regolamentazione uniforme si adatti poco alla realtà eterogenea dei Comuni ticinesi. Il Sindaco di Lugano, Michele Foletti, ha ricordato che diverse città hanno già adottato regolamenti specifici in materia di videosorveglianza, elaborati in funzione delle proprie esigenze e approvati dai rispettivi Consigli comunali. L'imposizione di una normativa generale, ha osservato, rischia di annullare la capacità decisionale locale e di appesantire inutilmente la gestione operativa.

Il Sindaco di Locarno, Nicola Pini, ha portato un esempio concreto: a Locarno un sistema di lettura delle targhe, utile sia per la gestione del traffico sia per la sicurezza, è stato disattivato su ordine cantonale per l'assenza di una base legale, con una perdita economica stimata in circa 100'000 franchi al mese. Questo episodio evidenzia, secondo Pini, i rischi concreti derivanti dalla mancanza di una normativa chiara e condivisa tra Cantone e Comuni.

Anche il Sindaco di Bellinzona, Mario Branda, ha espresso preoccupazione per una crescente tendenza alla centralizzazione, che ridurrebbe progressivamente l'autonomia comunale. Ha inoltre criticato la mancata consultazione preventiva, interpretata come segnale di scarsa considerazione istituzionale nei confronti delle autorità locali.

Infine, il Municipale di Mendrisio, Daniele Caverzasio, ha evidenziato le difficoltà operative che la nuova legge potrebbe comportare per i piccoli Comuni, spesso privi delle risorse necessarie per adeguarsi a una regolamentazione rigida e omogenea. Ha auspicato una maggiore attenzione all'impatto economico e amministrativo delle disposizioni previste, soprattutto in contesti con limitate capacità organizzative.

Nel complesso, dall'audizione è emersa una certa distanza tra le aspettative dei Comuni e l'impostazione adottata nella stesura delle leggi, in particolare per quanto riguarda il metodo di elaborazione, percepito da alcuni interlocutori come poco partecipativo.

La Commissione ha preso atto con attenzione delle critiche espresse dai rappresentanti dei Comuni, riconoscendo la legittimità delle preoccupazioni relative all'autonomia locale e al metodo adottato nella fase di elaborazione della normativa. Al contempo, ha ritenuto opportuno precisare alcuni elementi centrali del proprio approccio.

Anzitutto, è stato sottolineato come l'introduzione di una base legale cantonale rappresenti una necessità per offrire un quadro giuridico chiaro, stabile e uniforme a tutti i Comuni. In assenza di tale cornice, il rischio è quello di una proliferazione disomogenea di regolamenti locali, con potenziali contraddizioni normative e incertezze applicative.

La Commissione ha inoltre espresso rammarico per il mancato coinvolgimento formale degli attori comunali nelle fasi iniziali del processo legislativo. Proprio per questa ragione, alcuni relatori hanno ritenuto opportuno consultare singolarmente i rappresentanti di vari Comuni e successivamente tutta la Commissione ha deciso di approfondire la questione attraverso un'audizione collettiva.

È stato infine ricordato come esistano già sentenze del Tribunale federale – così come di tribunali di Stati europei, che fissano limiti chiari e stringenti all'utilizzo delle tecnologie di videosorveglianza, vincolando inevitabilmente anche la legislazione cantonale. La Commissione ha dunque inteso muoversi entro i margini ristretti lasciati dal diritto superiore, consapevole che la videosorveglianza può rappresentare uno strumento utile per il controllo del territorio, ma che non deve mai degenerare in una forma di controllo eccessivamente pervasivo, come evidenziato già nella premessa di questo rapporto.

4. RACCOMANDAZIONI COMMISSIONALI

Dopo le analisi di cui ai precedenti considerandi la commissione ha proposto queste modifiche:

Disegno di Legge proposto dal CdS	Disegno di Legge proposto dalla Commissione Costituzione e leggi
Art. 1 – Scopo ¹ La presente legge ha lo scopo di proteggere i diritti e le libertà fondamentali dei cittadini in relazione alla videosorveglianza pubblica e alle relative elaborazioni di dati personali.	Art. 1 – Scopo ¹ La presente legge ha lo scopo di proteggere i diritti e le libertà fondamentali dei cittadini in relazione alla videosorveglianza pubblica e alle relative elaborazioni di dati personali.
Art. 2 – Campo di applicazione ¹ La presente legge si applica a enti e istituzioni statali e parastatali cantonali e locali, alle Chiese e comunità religiose ufficialmente riconosciute dallo Stato e a privati che assumono compiti di diritto pubblico, qualora attuino la videosorveglianza sul demanio pubblico o su beni amministrativi per il mantenimento e la promozione della sicurezza e dell'ordine pubblico o per assicurare la logistica. ² Non soggiacciono alla presente legge, in particolare: a) gli organi di polizia cantonale e comunale che attuano la videosorveglianza pubblica in applicazione della legge sulla polizia del 12 dicembre 1989 (LPol) e della legge sulla collaborazione fra la polizia cantonale e le polizie comunali del 16 marzo 2011 (LCPol); b) gli organi di polizia che attuano la videosorveglianza in applicazione della legge sull'esecuzione delle pene e delle misure per gli adulti del 20 aprile 2020 (LEPM); c) gli enti e le istituzioni che attuano la videosorveglianza per scopi diversi da quelli previsti al capoverso ¹ .	Art. 2 – Campo di applicazione ¹ La presente legge si applica a enti e istituzioni statali e parastatali cantonali e locali, alle Chiese e comunità religiose ufficialmente riconosciute dallo Stato e a privati che assumono compiti di diritto pubblico, qualora attuino la videosorveglianza sul demanio pubblico o su beni amministrativi per il mantenimento e la promozione della sicurezza e dell'ordine pubblico o per assicurare la logistica. ² Non soggiacciono alla presente legge, in particolare: a) gli organi di polizia cantonale e comunale che attuano la videosorveglianza pubblica in applicazione della legge sulla polizia del 12 dicembre 1989 (LPol) e della legge sulla collaborazione fra la polizia cantonale e le polizie comunali del 16 marzo 2011 (LCPol); b) gli organi di polizia che attuano la videosorveglianza in applicazione della legge sull'esecuzione delle pene e delle misure per gli adulti del 20 aprile 2020 (LEPM); c) gli enti e le istituzioni che attuano la videosorveglianza per scopi diversi da quelli previsti al capoverso ¹ .
Art. 3 – Riserva di altre leggi ¹ Per aspetti delle elaborazioni di dati legate alla videosorveglianza pubblica che non sono disciplinati dalla presente legge, è applicabile la legge cantonale sulla protezione dei dati personali del 9 marzo 1987 (LPDP) e il relativo regolamento d'applicazione.	Art. 3 – Riserva di altre leggi ¹ Per aspetti delle elaborazioni di dati legate alla videosorveglianza pubblica che non sono disciplinati dalla presente legge, è applicabile la legge cantonale sulla protezione dei dati personali del 9 marzo 1987 (LPDP) e il relativo regolamento d'applicazione.

Rapporto n. 8282 R del 27 maggio 2025

Art. 4 – Definizioni

¹Ai sensi della presente legge, i seguenti termini significano:

- a) Titolare dell'elaborazione: autorità o organo che decide o legifera segnatamente in merito agli strumenti, agli scopi, all'estensione e alle modalità della sorveglianza pubblica, ai dati elaborati, alla durata di conservazione e alle misure di sicurezza.
- b) Videosorveglianza osservativa: attività di vigilare a distanza su un luogo pubblico, per una visione in tempo reale, in chiaro, con o senza registrazione d'immagini, allo scopo di monitorare e, se del caso, ripristinare il traffico di autoveicoli.
- c) Videosorveglianza dissuasiva: attività di vigilare a distanza, su un luogo, un bene amministrativo o un'infrastruttura pubblica, con registrazione e conservazione dei segnali d'immagine per una durata prestabilita. È finalizzata alla prevenzione di atti illeciti, di minacce o di turbamenti alla sicurezza o all'ordine pubblico, nonché alla ricostruzione e al perseguimento di infrazioni tramite analisi delle immagini.
- d) Videosorveglianza invasiva: attività di vigilare in tempo reale, in chiaro, con o senza registrazione d'immagini, allo scopo di gestire gli accessi di persone o veicoli a beni amministrativi o a strutture pubbliche.

Art. 5 – Videosorveglianza osservativa

¹Gli enti e le istituzioni responsabili di cui all'articolo 2 capoverso 1 possono sorvegliare in modalità osservativa un luogo accessibile al pubblico, se ciò è idoneo e necessario a garantire la supervisione e la gestione del traffico ai sensi dell'articolo 4 lettera b.

Art. 6 – Videosorveglianza dissuasiva

¹Gli enti e le istituzioni responsabili di cui all'articolo 2 capoverso 1 possono sorvegliare in modalità dissuasiva un luogo o un bene amministrativo accessibile al pubblico e conservare le relative immagini, se ciò è idoneo e necessario a garantire la prevenzione di turbamenti alla sicurezza o all'ordine pubblico e a ricostruire, se del caso, le responsabilità.

²Le immagini possono essere analizzate successivamente a un evento rilevante per la sicurezza o l'ordine pubblico, per la ricostruzione di responsabilità e per il perseguimento di reati.

³L'introduzione della videosorveglianza dissuasiva deve essere preceduta da una valutazione dell'idoneità, dell'efficacia e della necessità della misura per garantire la sicurezza o l'ordine pubblico,

Art. 4 – Definizioni

¹Ai sensi della presente legge, i seguenti termini significano:

- a) Titolare dell'elaborazione: autorità o organo che decide o legifera segnatamente in merito agli strumenti, agli scopi, all'estensione e alle modalità della sorveglianza pubblica, ai dati elaborati, alla durata di conservazione e alle misure di sicurezza.
- b) **Mandatario: responsabile dell'elaborazione e del trattamento dei dati su mandato del titolare dell'elaborazione.**
- c) ~~b)~~ Videosorveglianza osservativa: attività di vigilare a distanza su un luogo pubblico, per una visione in tempo reale, in chiaro, con o senza registrazione d'immagini, allo scopo di monitorare e, se del caso, ripristinare il traffico di autoveicoli.
- d) ~~e)~~ Videosorveglianza dissuasiva: attività di vigilare a distanza, su un luogo, un bene amministrativo o un'infrastruttura pubblica, con registrazione e conservazione dei segnali d'immagine per una durata prestabilita. È finalizzata alla prevenzione di atti illeciti, di minacce o di turbamenti alla sicurezza o all'ordine pubblico, nonché alla ricostruzione e al perseguimento di infrazioni tramite analisi delle immagini.
- e) ~~d)~~ Videosorveglianza invasiva: attività di vigilare in tempo reale, in chiaro, con o senza registrazione d'immagini, allo scopo di gestire gli accessi di persone o veicoli a beni amministrativi o a strutture pubbliche.

Art. 5 – Videosorveglianza osservativa

¹Gli enti e le istituzioni responsabili di cui all'articolo 2 capoverso 1 possono sorvegliare in modalità osservativa un luogo accessibile al pubblico, se ciò è idoneo e necessario a garantire la supervisione e la gestione del traffico ai sensi dell'articolo 4 lettera c.

²È consentita unicamente la videosorveglianza priva di registrazione audio e senza l'impiego di applicativi / strumenti informatici per il riconoscimento automatico e il tracciamento automatizzato delle persone.

Art. 6 – Videosorveglianza dissuasiva

¹Gli enti e le istituzioni responsabili di cui all'articolo 2 capoverso 1 possono sorvegliare in modalità dissuasiva un luogo o un bene amministrativo accessibile al pubblico e conservare le relative immagini, se ciò è idoneo e necessario a garantire la prevenzione di turbamenti alla sicurezza o all'ordine pubblico e a ricostruire, se del caso, le responsabilità.

²Le immagini possono essere analizzate successivamente a un evento rilevante per la sicurezza o l'ordine pubblico, per la ricostruzione di responsabilità e per il perseguimento di reati.

³L'introduzione della videosorveglianza dissuasiva deve essere preceduta da una valutazione dell'idoneità e dell'efficacia della misura.

Rapporto n. 8282 R del 27 maggio 2025

da un'analisi d'impatto sui diritti e sulle libertà del cittadino e da una lista di misure idonee a eliminare o ridurre tali rischi. ⁴La videosorveglianza dissuasiva non si giustifica, in particolare, quando: a) gli scopi perseguiti possono essere pienamente raggiunti anche con l'ausilio di misure meno incisive nei diritti delle persone, ma altrettanto efficaci per il raggiungimento dello scopo; b) avviene alla ricerca di possibili reati, in assenza di un sospetto concreto, oppure implica la raccolta preventiva di dati, senza che vi sia un chiaro e concreto scopo di elaborazione.	⁴La videosorveglianza dissuasiva non si giustifica, in particolare, quando: a) gli scopi perseguiti possono essere pienamente raggiunti anche con l'ausilio di misure meno incisive nei diritti delle persone, ma altrettanto efficaci per il raggiungimento dello scopo; b) avviene alla ricerca di possibili reati, in assenza di un sospetto concreto, oppure implica la raccolta preventiva di dati, senza che vi sia un chiaro e concreto scopo di elaborazione. ⁵È consentita unicamente la videosorveglianza priva di registrazione audio e senza l'impiego di applicativi / strumenti informatici per il riconoscimento automatico e il tracciamento automatizzato delle persone.
Art. 7 – Videosorveglianza invasiva ¹Gli enti e le istituzioni responsabili di cui all'articolo 2 capoverso 1 possono sorvegliare in modalità invasiva l'accesso a beni amministrativi pubblici, se ciò è idoneo e necessario a gestire gli accessi ai sensi dell'articolo 4 lettera d.	Art. 7 – Videosorveglianza invasiva ¹Gli enti e le istituzioni responsabili di cui all'articolo 2 capoverso 1 possono sorvegliare in modalità invasiva l'accesso a beni amministrativi pubblici, se ciò è idoneo e necessario a gestire gli accessi ai sensi dell'articolo 4 lettera e. ²È consentita la registrazione audio ma non l'impiego di applicativi / strumenti per il riconoscimento automatico e il tracciamento automatizzato delle persone.
Art. 8 – Finalità ¹I dati personali non possono essere utilizzati per scopi che esulano da quelli previsti dagli articoli 5-7 della presente legge.	Art. 8 – Finalità ¹I dati personali non possono essere utilizzati per scopi che esulano da quelli previsti dagli articoli 5-7 della presente legge. ²La raccolta indiscriminata di dati (fishing expedition) è vietata. Il trattamento dei dati deve avvenire nel rispetto dei principi di necessità, proporzionalità e finalità chiaramente definite.
Art. 9 – Proporzionalità ¹La videosorveglianza deve essere proporzionata, in particolare per quanto riguarda lo scopo perseguito, gli strumenti utilizzati, le modalità di attuazione, l'estensione territoriale e temporale e la cerchia di personale abilitato alla gestione e all'accesso agli impianti di videosorveglianza, ai programmi informatici ivi correlati e alle immagini registrate. ²Nella misura in cui è tecnicamente e finanziariamente realizzabile, beni o interessi protetti sono schermati da filtri della privacy. ³La proporzionalità della videosorveglianza deve essere periodicamente rivalutata.	Art. 9 – Proporzionalità ¹La videosorveglianza deve essere proporzionata, in particolare per quanto riguarda lo scopo perseguito, gli strumenti utilizzati, le modalità di attuazione, l'estensione territoriale e temporale e la cerchia di personale abilitato alla gestione e all'accesso agli impianti di videosorveglianza, ai programmi informatici ivi correlati e alle immagini registrate. ²Nella misura in cui è tecnicamente e finanziariamente realizzabile, beni o interessi protetti sono schermati da filtri della privacy. ³La proporzionalità della videosorveglianza deve essere valutata prima dell'implementazione e periodicamente rivalutata.
Art. 10 – Esattezza ¹Il titolare deve garantire l'esattezza dei dati elaborati, in particolare la correttezza, l'autenticità, la veridicità e la completezza.	Art. 10 – Esattezza ¹Il titolare deve garantire l'esattezza dei dati elaborati, in particolare la correttezza, l'autenticità, la veridicità e la completezza.

Rapporto n. 8282 R del 27 maggio 2025

Art. 11 – Trasparenza

¹Il titolare garantisce un'adeguata informazione sulla videosorveglianza, segnatamente con cartelli indicatori possibilmente prima dell'entrata nel campo di visione delle singole videocamere e in prossimità delle stesse

²L'informazione concerne perlomeno la presenza della videocamera, il titolare e la base legale.

³In caso di videosorveglianza del sedime scolastico, gli allievi e/o i loro rappresentanti legali devono essere informati in modo adeguato, trasparente e completo anche sulle tempistiche, sui luoghi e sulle modalità della videosorveglianza.

Art. 12 – Sicurezza dei dati

¹I titolari e gli eventuali mandatarî devono garantire, sin dalla progettazione di un sistema di videosorveglianza pubblica, l'integrità, la disponibilità, la confidenzialità e l'autenticità dei dati elaborati tramite adeguate misure tecniche e organizzative. In particolare, devono proteggere i dati contro la perdita, l'abuso e il danneggiamento.

²Le misure tecniche e organizzative devono essere adeguate allo stato della tecnica, alla natura e all'estensione dell'elaborazione dei dati come pure al grado di probabilità e di gravità del rischio che l'elaborazione implica.

³In particolare, devono essere limitati gli accessi alle registrazioni tramite credenziali di accesso personalizzate, disponibili unicamente al personale autorizzato e devono essere giornalizzati gli accessi per la ricostruzione di eventi o responsabilità legate a possibili abusi dei dati.

Art. 13 – Disposizioni materiali e vigilanza

¹Il titolare emana le disposizioni materiali necessarie all'esecuzione della presente legge. Definisce, in particolare:

- a) lo scopo della videosorveglianza;
- b) la tipologia di strumenti di videosorveglianza da utilizzare;
- c) il mandato di esecuzione della videosorveglianza;
- d) i luoghi soggetti a videosorveglianza;
- e) le modalità e le condizioni della videosorveglianza;
- f) la durata di conservazione dei dati;
- g) i diritti di accesso ai dati;
- h) le misure di sicurezza.

²Vigila sulla corretta applicazione e sul rispetto della presente legge e delle disposizioni materiali d'esecuzione.

Art. 11 – Trasparenza

¹Il titolare garantisce un'adeguata informazione sulla videosorveglianza, segnatamente con cartelli indicatori possibilmente prima dell'entrata nel campo di visione delle singole videocamere e in prossimità delle stesse

²L'informazione concerne **almeno** la presenza della videocamera, il titolare e la base legale.

³In caso di videosorveglianza del sedime scolastico, gli allievi e/o i loro rappresentanti legali devono essere informati in modo adeguato, trasparente e completo anche sulle tempistiche, sui luoghi e sulle modalità della videosorveglianza.

Art. 12 – Sicurezza dei dati

¹I titolari e gli eventuali mandatarî devono garantire, sin dalla progettazione di un sistema di videosorveglianza pubblica, l'integrità, la disponibilità, la confidenzialità e l'autenticità dei dati elaborati tramite adeguate misure tecniche e organizzative. In particolare, devono proteggere i dati contro la perdita, l'abuso e il danneggiamento.

²Le misure tecniche e organizzative devono essere adeguate allo stato della tecnica, alla natura e all'estensione dell'elaborazione dei dati come pure al grado di probabilità e di gravità del rischio che l'elaborazione implica.

³In particolare, devono essere limitati gli accessi alle registrazioni tramite credenziali di accesso personalizzate, disponibili unicamente al personale autorizzato e devono essere giornalizzati gli accessi per la ricostruzione di eventi o responsabilità legate a possibili abusi dei dati.

Art. 13 – Disposizioni materiali e vigilanza

¹Il titolare emana le disposizioni materiali necessarie all'esecuzione della presente legge. Definisce, in particolare:

- a) lo scopo della videosorveglianza;
- b) la tipologia di strumenti di videosorveglianza da utilizzare;
- c) il mandato di esecuzione della videosorveglianza;
- d) i luoghi soggetti a videosorveglianza;
- e) le modalità e le condizioni della videosorveglianza;
- f) la durata di conservazione dei dati;
- g) i diritti di accesso ai dati;
- h) le misure di sicurezza.

²Vigila **periodicamente** sulla corretta applicazione e sul rispetto della presente legge e delle disposizioni materiali d'esecuzione.

Rapporto n. 8282 R del 27 maggio 2025

Art. 14 – Trasmissione di dati a terzi ¹Di principio, le registrazioni non sono trasmesse a terzi. ²Rimane riservata la collaborazione tra polizie sulla base di specifiche norme di assistenza amministrativa. ³Nel caso di procedimenti civili, penali o amministrativi, le registrazioni possono essere trasmesse alle competenti autorità, nella misura in cui ciò sia necessario a titolo di prova. I dati personali di terzi non interessati dal procedimento sono resi anonimi.	Art. 14 – Trasmissione di dati a terzi ¹Di principio, le registrazioni non sono trasmesse a terzi. ²Rimane riservata la collaborazione tra polizie sulla base di specifiche norme di assistenza amministrativa. ³Nel caso di procedimenti civili, penali o amministrativi, le registrazioni possono essere trasmesse alle competenti autorità, nella misura in cui ciò sia necessario a titolo di prova. I dati personali di terzi non interessati dal procedimento sono resi anonimi. ⁴Le richieste di accesso e le operazioni di elaborazione dei dati devono essere tracciabili e conformi alle disposizioni applicabili.
Art. 15 – Conservazione, archiviazione e distruzione dei dati ¹Le registrazioni possono essere conservate per una durata massima di 100 giorni, decorsi i quali vanno distrutti. ²Rimane riservata la conservazione da parte del titolare di una copia delle registrazioni in caso di procedura civile, penale o amministrativa, fino a conclusione della stessa.	Art. 15 – Conservazione, archiviazione e distruzione dei dati ¹Le registrazioni sono conservate fintanto che siano date specifiche e obiettive esigenze di utilizzazione e che, pertanto, siano necessarie per gli scopi per i quali sono state lecitamente raccolte o elaborate. ²Rimane riservata la conservazione da parte del titolare di una copia delle registrazioni in caso di procedura civile, penale o amministrativa, fino a conclusione della stessa. ³Al termine del periodo di conservazione, i dati devono essere cancellati in modo automatico e definitivo tramite sistemi idonei a garantirne l'irrecuperabilità.
	Art. 16 – Disposizioni penali ¹Si rinvia al diritto penale federale. Le infrazioni sono perseguite secondo il diritto penale federale applicabile
Art. 16 – Entrata in vigore ¹La presente legge sottostà a referendum facoltativo. ²Il Consiglio di Stato ne fissa l'entrata in vigore.	Art. 17 – Entrata in vigore ¹La presente legge sottostà a referendum facoltativo. ²Il Consiglio di Stato ne fissa l'entrata in vigore.

Commento ai singoli articoli

Articolo 1 – Scopo La formulazione dell'articolo resta invariata rispetto alla proposta del Consiglio di Stato. La Commissione ha condiviso l'impostazione generale, ritenendo importante ribadire fin dall'inizio che lo scopo della legge è quello di proteggere i diritti e le libertà fondamentali dei cittadini in relazione all'uso della videosorveglianza. Nessuna modifica necessaria.

Articolo 2 – Campo di applicazione La Commissione ha confermato il testo proposto dal Consiglio di Stato, ritenendolo sufficientemente chiaro nel definire l'ambito soggettivo e oggettivo di applicazione della legge. Si è condiviso il principio per cui determinati ambiti, in particolare le attività della polizia disciplinate da leggi settoriali (legge che è attualmente in revisione), restano esclusi dal campo di applicazione della presente legge.

Articolo 3 – Riserva di altre leggi Anche in questo caso, la Commissione ha accolto favorevolmente la formulazione del Consiglio di Stato, ritenendola coerente con

l'impostazione normativa generale: per tutti gli aspetti non trattati specificamente, si applica la LPDP cantonale.

Articolo 4 – Definizioni La Commissione ha ritenuto opportuno ampliare il catalogo delle definizioni inserendo la figura del "mandatario", responsabile dell'elaborazione dei dati per conto del titolare. Tale inserimento rafforza la chiarezza interpretativa e operativa della legge, anche se il termine è già presente nella LPDP. La definizione è stata uniformata terminologicamente alla lettera a), specificando: "Mandatario: responsabile dell'elaborazione e del trattamento dei dati su mandato del titolare dell'elaborazione."

Articolo 5 – Videosorveglianza osservativa La Commissione ha introdotto un importante elemento di tutela: il divieto di registrazione audio e l'impiego di strumenti di riconoscimento/tracciamento automatizzato. Tale precisazione garantisce che questa forma di sorveglianza resti proporzionata alla sua finalità (gestione del traffico). Per coerenza lessicale, è stato preferito il termine "applicativi / strumenti informatici". È stato inoltre corretto il rinvio interno all'art. 4 lett. c), per adeguarlo all'inserimento della nuova definizione di mandatario.

Articolo 6 – Videosorveglianza dissuasiva. Sono stati introdotti ulteriori livelli di garanzia, tra cui il divieto di registrazione audio e di tracciamento, l'obbligo di una valutazione ex ante dell'efficacia della misura, nonché la consultazione preventiva dell'ICPD in presenza di un rischio elevato per i diritti fondamentali. La formulazione della norma è stata inoltre armonizzata per rafforzarne la chiarezza giuridica e rendere obbligatoria la consultazione.

Articolo 7 – Videosorveglianza invasiva Si è mantenuta la possibilità di registrazione audio, considerata coerente con la gestione degli accessi, ma vietato l'uso di tecnologie invasive. È stato inoltre corretto il rinvio interno all'art. 4 lett. e), per adeguarlo all'inserimento della nuova definizione di mandatario.

Articolo 8 – Finalità La Commissione ha introdotto un'innovazione rilevante: il divieto espresso di "fishing expedition" (segnatamente una raccolta indiscriminata e generalizzata di immagini o dati personali, senza una finalità specifica, concreta e giustificata) e il richiamo formale ai principi di necessità, proporzionalità e finalità specifica.

Articolo 9 – Proporzionalità Si specifica che la proporzionalità deve essere valutata anche ex ante. La Commissione ha considerato opportuno menzionare, nel rapporto, l'opportunità di consultare l'ICPD nei casi in cui le misure appaiano sproporzionate, pur senza introdurre un vincolo normativo esplicito.

Articolo 10 – Esattezza La disposizione è stata confermata senza modifiche. La Commissione ha sottolineato l'importanza del principio, specie in un contesto in cui le informazioni raccolte possono avere rilevanza probatoria.

Articolo 11 – Trasparenza È stato introdotto l'avverbio "almeno" al posto di "perlomeno" al cpv. 2 per chiarire che gli elementi informativi elencati costituiscono un minimo obbligatorio. Ciò permette una maggiore flessibilità applicativa, mantenendo un adeguato livello di tutela per la cittadinanza.

Articolo 12 – Sicurezza dei dati La Commissione ha condiviso appieno le disposizioni proposte dal Consiglio di Stato. Particolarmente rilevante l'obbligo di accessi tracciabili tramite credenziali personalizzate.

Articolo 13 – Disposizioni materiali e vigilanza È stata aggiunta l'espressione "vigilanza periodica", per sottolineare la necessità di controlli regolari. La formulazione è stata ritenuta efficace e rispettosa del principio di buon governo.

Articolo 14 – Trasmissione di dati a terzi La Commissione ha rafforzato la norma prevedendo la tracciabilità delle richieste e delle elaborazioni. È stata proposta una formulazione più giuridicamente precisa: "Le richieste di accesso e le operazioni di elaborazione dei dati devono essere registrate in modo tracciabile e conforme alle disposizioni applicabili."

Articolo 15 – Conservazione, archiviazione e distruzione dei dati si è ritenuto opportuno riformulare il principio di durata per renderlo conforme ai criteri di necessità e finalità. Si è quindi preferito evitare un termine fisso di 100 giorni (in considerazione della giurisprudenza precedentemente esposta), optando per un approccio flessibile: "Le registrazioni sono conservate per il tempo strettamente necessario...". Inoltre si è rafforzato anche l'obbligo di cancellazione automatica e definitiva, con garanzia di irrecoverabilità.

Articolo 16 – Disposizioni penali Si è deciso di rinviare al diritto penale federale, ritenendo che l'inserimento di sanzioni specifiche cantonali non sia indispensabile. La scelta consente uniformità e coerenza normativa con altri Cantoni.

Articolo 17 – Entrata in vigore Testo confermato senza modifiche. La legge sarà sottoposta a referendum facoltativo.

5. CONCLUSIONI

Come ampiamente illustrato nell'introduzione, il confronto politico su come gestire i sistemi tecnologici di sorveglianza della popolazione si inserisce in un vivace dibattito culturale – avviato oltre un secolo fa e declinato in racconti, romanzi, film e videogiochi.

In più punti del rapporto, la Commissione ha ribadito la piena consapevolezza degli aspetti critici connessi a uno strumento come la videosorveglianza, in particolare sotto il profilo della tutela della sfera privata. La scelta di fondo è stata quella di seguire con rigore e ragionevolezza i limiti fissati dal diritto superiore, per evitare che il legittimo bisogno di controllo del territorio si trasformi in una lesione degli spazi di vita riservati agli individui. Degno di nota, in tal senso, è l'emendamento all'art. 7, che vieta esplicitamente l'impiego in Ticino di applicativi per il riconoscimento facciale e il tracciamento automatizzato delle persone.

La rapida evoluzione dell'intelligenza artificiale è, sotto questo profilo, un elemento da non sottovalutare. La velocità dell'innovazione tecnologica – evidente anche nel breve arco di tempo trascorso dalla stesura del rapporto – impone di considerare un necessario margine di imprevedibilità. La Commissione è conscia che queste norme rappresentano un punto

di partenza e non di arrivo, costruite su una realtà in rapido mutamento, che richiederà inevitabilmente aggiornamenti e adattamenti continui.

Dal punto di vista procedurale, la Commissione ha voluto valorizzare il coinvolgimento dei rappresentanti dei Comuni nell'analisi del messaggio del Consiglio di Stato. Il dialogo, in particolare con i sindaci dei centri urbani, ha consentito di raccogliere indicazioni preziose, dando luogo anche a un confronto schietto con i limiti imposti sia dal diritto superiore, sia dalla giurisprudenza già consolidata in materia di videosorveglianza. In tal senso, è opportuno rinnovare l'invito al Consiglio di Stato affinché in futuro, su progetti normativi che toccano direttamente l'autonomia comunale, il coinvolgimento dei Municipi sia più tempestivo e il confronto più aperto.

In conclusione, la nuova Legge sulla videosorveglianza pubblica rappresenta un passo necessario, che dota il nostro Cantone di un quadro giuridico chiaro, stabile e uniforme – a beneficio dei Comuni e della cittadinanza. Essa consente di prevenire la frammentazione normativa e le incertezze applicative che potrebbero derivare da una proliferazione di regolamenti locali. Sarà comunque compito di Governo e Parlamento monitorare con attenzione le future evoluzioni – normative e tecnologiche – per evitare che queste regole diventino rapidamente superate.

Visto quanto precede, si propone al Gran Consiglio di approvare l'allegato disegno di legge.

Per la Commissione Costituzione e leggi:

Simona Genini, Lara Filippini e Alessandro Corti, relatori

Balli - Boscolo (con riserva) - Capoferri -

Censi - Genini Sem - Giudici - Ghisolfi -

Lepori - Ortelli P. - Padlina - Passardi -

Petralli (con riserva) - Ponti - Terraneo

Rapporto n. 8282 R del 27 maggio 2025

Disegno di

**Legge
sulla videosorveglianza pubblica
(LViSo)
del**

**IL GRAN CONSIGLIO
DELLA REPUBBLICA E CANTONE TICINO**

- visto il messaggio del Consiglio di Stato n. 8282 del 17 maggio 2023,
- visto il rapporto della Commissione Costituzione e leggi n. 8282R del 27 maggio 2025;

decreta:

Capitolo primo
Norme generali e definizioni

Scopo

Art. 1

La presente legge ha lo scopo di proteggere i diritti e le libertà fondamentali dei cittadini in relazione alla videosorveglianza pubblica e alle relative elaborazioni di dati personali.

Campo di applicazione

Art. 2

¹La presente legge si applica a enti e istituzioni statali e parastatali cantonali e locali, alle Chiese e comunità religiose ufficialmente riconosciute dallo Stato e a privati che assumono compiti di diritto pubblico, qualora attuino la videosorveglianza sul demanio pubblico o su beni amministrativi per il mantenimento e la promozione della sicurezza e dell'ordine pubblico o per assicurare la logistica.

²Non soggiacciono alla presente legge, in particolare:

- a) gli organi di polizia cantonale e comunale che attuano la videosorveglianza pubblica in applicazione della legge sulla polizia del 12 dicembre 1989 (LPol) e della legge sulla collaborazione fra la polizia cantonale e le polizie comunali del 16 marzo 2011 (LCPol);
- b) gli organi di polizia che attuano la videosorveglianza in applicazione della legge sull'esecuzione delle pene e delle misure per gli adulti del 20 aprile 2020 (LEPM);
- c) gli enti e le istituzioni che attuano la videosorveglianza per scopi diversi da quelli previsti al capoverso 1.

Riserva di altre leggi

Art. 3

Per aspetti delle elaborazioni di dati legate alla videosorveglianza pubblica che non sono disciplinati dalla presente legge, è applicabile la legge cantonale sulla protezione dei dati personali del 9 marzo 1987 (LPDP) e il relativo regolamento d'applicazione.

Definizioni

Art. 4

Ai sensi della presente legge, i seguenti termini significano:

- a) *titolare dell'elaborazione*: autorità o organo che decide o legifera segnatamente in merito agli strumenti, agli scopi, all'estensione e alle modalità della sorveglianza pubblica, ai dati elaborati, alla durata di conservazione e alle misure di sicurezza. Inoltre, è organo che vigila sull'applicazione della presente legge e che risponde in caso di violazione;
- b) *mandatario*: responsabile dell'elaborazione e del trattamento dei dati su mandato del titolare dell'elaborazione.
- c) *videosorveglianza osservativa*: attività di vigilare a distanza su un luogo pubblico, per una visione in tempo reale, in chiaro, con o senza registrazione d'immagini, allo scopo di monitorare e, se del caso, ripristinare il traffico di autoveicoli;
- d) *videosorveglianza dissuasiva (o preventiva e repressiva)*: attività di vigilare a distanza, su un luogo, un bene amministrativo o un'infrastruttura pubblica, con registrazione e conservazione dei segnali d'immagine per una durata prestabilita. È finalizzata alla prevenzione di atti illeciti, di minacce o di turbamenti alla sicurezza o all'ordine pubblico, tramite la posa ben riconoscibile di videocamere di sorveglianza, nonché alla ricostruzione e al perseguimento di infrazioni tramite analisi delle immagini successiva alla loro commissione;
- e) *videosorveglianza invasiva*: attività di vigilare in tempo reale, in chiaro, con o senza registrazione d'immagini, allo scopo di gestire gli accessi di persone o veicoli a beni amministrativi o a strutture pubbliche.

Capitolo secondo

Modalità della videosorveglianza

Videosorveglianza osservativa

Art. 5

¹Gli enti e le istituzioni responsabili di cui all'articolo 2 capoverso 1 possono sorvegliare in modalità osservativa un luogo accessibile al pubblico, se ciò è idoneo e necessario a garantire la supervisione e la gestione del traffico ai sensi dell'articolo 4 lettera c.

²È consentita unicamente la videosorveglianza priva di registrazione audio e senza l'impiego di applicativi/strumenti informatici per il riconoscimento automatico e il tracciamento automatizzato delle persone.

Videosorveglianza dissuasiva

Art. 6

¹Gli enti e le istituzioni responsabili di cui all'articolo 2 capoverso 1 possono sorvegliare in modalità dissuasiva un luogo o un bene amministrativo accessibile al pubblico e conservare le relative immagini, se ciò è idoneo e necessario a garantire la prevenzione di turbamenti alla sicurezza o all'ordine pubblico e a ricostruire, se del caso, le responsabilità.

²Le immagini possono essere analizzate successivamente a un evento rilevante per la sicurezza o l'ordine pubblico, per la ricostruzione di responsabilità e per il perseguimento di reati.

³L'introduzione della videosorveglianza dissuasiva deve essere preceduta da una valutazione dell'idoneità e dell'efficacia della misura.

⁴La videosorveglianza dissuasiva non si giustifica, in particolare, quando:

a) gli scopi perseguiti possono essere pienamente raggiunti anche con l'ausilio di misure meno incisive nei diritti delle persone, ma altrettanto efficaci per il raggiungimento dello scopo;

b) avviene alla ricerca di possibili reati, in assenza di un sospetto concreto, oppure implica la raccolta preventiva di dati, senza che vi sia un chiaro e concreto scopo di elaborazione.

⁵È consentita unicamente la videosorveglianza priva di registrazione audio e senza l'impiego di applicativi/strumenti informatici per il riconoscimento automatico e il tracciamento automatizzato delle persone.

Videosorveglianza invasiva

Art. 7

¹Gli enti e le istituzioni responsabili di cui all'articolo 2 capoverso 1 possono sorvegliare in modalità invasiva l'accesso a beni amministrativi pubblici, se ciò è idoneo e necessario a gestire gli accessi ai sensi dell'articolo 4 lettera e.

²È consentita la registrazione audio ma non l'impiego di applicativi/strumenti per il riconoscimento automatico e il tracciamento automatizzato delle persone.

Capitolo terzo

Principi generali

Finalità

Art. 8

¹I dati personali non possono essere utilizzati per scopi che esulano da quelli previsti dagli articoli 5-7 della presente legge.

²La raccolta indiscriminata di dati (fishing expedition) è vietata. Il trattamento dei dati deve avvenire nel rispetto dei principi di necessità, proporzionalità e finalità chiaramente definite.

Proporzionalità

Art. 9

¹La videosorveglianza deve essere proporzionata, in particolare per quanto riguarda lo scopo perseguito, gli strumenti utilizzati, le modalità di attuazione, l'estensione territoriale e temporale e la cerchia di personale abilitato alla gestione e all'accesso agli impianti di videosorveglianza, ai programmi informatici ivi correlati e alle immagini registrate.

²Nella misura in cui è tecnicamente e finanziariamente realizzabile, beni o interessi protetti sono schermati da filtri della privacy.

³La proporzionalità della videosorveglianza deve essere valutata prima dell'implementazione e periodicamente rivalutata.

Esattezza

Art. 10

Il titolare deve garantire l'esattezza dei dati elaborati, in particolare la correttezza, l'autenticità, la veridicità e la completezza.

Trasparenza

Art. 11

¹Il titolare garantisce un'adeguata informazione sulla videosorveglianza, segnatamente con cartelli indicatori possibilmente prima dell'entrata nel campo di visione delle singole videocamere e in prossimità delle stesse.

²L'informazione concerne almeno la presenza della videocamera, il titolare e la base legale.

³In caso di videosorveglianza del sedime scolastico, gli allievi e/o i loro rappresentanti legali devono essere informati in modo adeguato, trasparente e completo anche sulle tempistiche, sui luoghi e sulle modalità della videosorveglianza.

Sicurezza dei dati

Art. 12

¹I titolari e gli eventuali mandatarî devono garantire, sin dalla progettazione di un sistema di videosorveglianza pubblica, l'integrità, la disponibilità, la confidenzialità e l'autenticità dei dati elaborati tramite adeguate misure tecniche e organizzative. In particolare, devono proteggere i dati contro la perdita, l'abuso e il danneggiamento.

²Le misure tecniche e organizzative devono essere adeguate allo stato della tecnica, alla natura e all'estensione dell'elaborazione dei dati come pure al grado di probabilità e di gravità del rischio che l'elaborazione implica.

³In particolare, devono essere limitati gli accessi alle registrazioni tramite credenziali di accesso personalizzate, disponibili unicamente al personale autorizzato e devono essere giornalizzati gli accessi per la ricostruzione di eventi o responsabilità legate a possibili abusi dei dati.

Capitolo quarto

Organizzazione, trasmissione e archiviazione dei dati

Disposizioni materiali e vigilanza

Art. 13

¹Il titolare emana le disposizioni materiali necessarie all'esecuzione della presente legge. Definisce, in particolare:

- a) lo scopo della videosorveglianza;
- b) la tipologia di strumenti di videosorveglianza da utilizzare;
- c) il mandato di esecuzione della videosorveglianza;
- d) i luoghi soggetti a videosorveglianza;
- e) le modalità e le condizioni della videosorveglianza;
- f) la durata di conservazione dei dati;
- g) i diritti di accesso ai dati;
- h) le misure di sicurezza.

²Vigila periodicamente sulla corretta applicazione e sul rispetto della presente legge e delle disposizioni materiali d'esecuzione.

Trasmissione di dati a terzi

Art. 14

¹Di principio, le registrazioni non sono trasmesse a terzi.

²Rimane riservata la collaborazione tra polizie sulla base di specifiche norme di assistenza amministrativa.

³Nel caso di procedimenti civili, penali o amministrativi, le registrazioni possono essere trasmesse alle competenti autorità, nella misura in cui ciò sia necessario a titolo di prova. I dati personali di terzi non interessati dal procedimento sono resi anonimi.

⁴Le richieste di accesso e le operazioni di elaborazione dei dati devono essere tracciabili e conformi alle disposizioni applicabili.

Conservazione, archiviazione e distruzione dei dati

Art. 15

¹Le registrazioni sono conservate fintanto che siano date specifiche e obiettive esigenze di utilizzazione e che, pertanto, siano necessarie per gli scopi per i quali sono state lecitamente raccolte o elaborate.

²Rimane riservata la conservazione da parte del titolare di una copia delle registrazioni in caso di procedura civile, penale o amministrativa, fino a conclusione della stessa.

³Al termine del periodo di conservazione, i dati devono essere cancellati in modo automatico e definitivo tramite sistemi idonei a garantirne l'irrecuperabilità.

Disposizioni penali

Art. 16

Le infrazioni sono perseguite secondo il diritto penale federale applicabile.

Capitolo quinto

Disposizioni finali

Entrata in vigore

Art. 17

¹La presente legge sottostà a referendum facoltativo.

²Il Consiglio di Stato ne fissa l'entrata in vigore.