RIVISTA TICINESE DI DIRITTO

I - 2022

CANCELLERIA DELLO STATO DEL CANTONE TICINO
HELBING LICHTENHAHN

ESTRATTO

RIVISTA TICINESE
DI DIRITTO

I- 2022

Giordano Costa

Videosorveglianza, riconoscimento facciale e altre tecnologie di controllo pubblico in Ticino, tra sicurezza e libertà

CANCELLERIA DELLO STATO DEL CANTONE TICINO
HELBING LICHTENHAHN

Direzione e responsabilità editoriale:
Prof. Dr. Marco Borghi
e-mail: marco.borghi@unifr.ch

Redazione della parte fiscale:
Dr. Andrea Pedroli, Presidente della Camera di diritto tributario
e-mail: andrea.pedroli@ti.ch

incaricati dal Consiglio di Stato

Edita da: Cancelleria dello Stato del Cantone Ticino e
Helbing Lichtenhahn, Basilea (www.helbing.ch)

Distribuzione: – Servizi giuridici del Consiglio di Stato,
6501 Bellinzona (e-mail: legislazione@ti.ch)
– Schweizer Buchzentrum, Industriestrasse Ost, 4614 Hägendorf

Coordinamento e allestimento: Gibi Borghi
e-mail: borghi.gibi@bluewin.ch

Stampa: Salvioni arti grafiche, 6500 Bellinzona
e-mail: info@salvioni.ch

Copertina: riproduzione da Cornelia Forster

ISSN 1661-0954 – ISBN 978-3-7190-4621-7 (Helbing Lichtenhahn)
ISBN 978-88-6303-057-0 (Repubblica e Cantone Ticino)

Videosorveglianza, riconoscimento facciale e altre tecnologie di controllo pubblico in Ticino, tra sicurezza e libertà

Con primi spunti normativi per una nuova legge cantonale quadro sulla sorveglianza pubblica

Giordano Costa[*]

---

[*] Lic. iur., Incaricato cantonale della protezione dei dati. L'autore si esprime a titolo personale e non ingaggia la responsabilità dello Stato. Nessuna informazione raccolta, valutata o prodotta in seno al Gruppo di lavoro sulla sorveglianza pubblica in Ticino, istituito dal Consiglio di Stato alla fine del 2020 e coordinato dallo scrivente, è confluita nel presente contributo.

Premessa

La si considera una conquista oramai definitiva e consolidata, nelle nostre moderne società. Ma, oggi come in passato, la libertà è minacciata. In ambito tecnologico, vi rinunciamo spesso con leggerezza, pur di continuare a beneficiare dei vantaggi delle nuove tecnologie. Come è stato detto all'apertura dei lavori di un convegno sulla società sorvegliata, tenutosi a Roma nel 2016 in occasione della giornata europea della privacy sotto l'egida del Garante italiano per la protezione dei dati personali – e le cui affermazioni sono ancora del tutto attuali – *«… nell'esperienza quotidiana siamo bersagliati, con un misto di nostra meraviglia e ammirazione, da nuovi servizi e nuove applicazioni, e poiché nella dimensione digitale l'integrità fisica è rispettata, la percezione dei rischi per le no-*

stre persone è praticamente inesistente»[1]. L'assenza di percezione di questi rischi è riconoscibile anche nell'ambito della videosorveglianza e del controllo pubblico, a volte a tal punto che il valore della libertà sembra soccombere alla ragione di sicurezza. Perciò *«… anche se alcune tecnologie come la videosorveglianza sembrano oramai fare parte del corredo urbano, esse devono essere utilizzate nella maniera più utile in termini di prevenzione e più sostenibile sotto il profilo democratico»*[2]. Quando si parla di videosorveglianza o di altre forme di controllo pubblico, bisogna perciò sempre e con insistenza parlare anche di democrazia e di libertà e impedire che le strategie di sicurezza degenerino in sorveglianza massiva. Il discorso democratico e di diritto s'impone a maggior ragione per il fatto che i moderni strumenti di sorveglianza non permettono più soltanto il presidio tecnico grandangolare di un determinato perimetro di sedime pubblico in modalità dissuasiva, ma si sono evoluti verso forme sempre più performanti e incisive nei diritti e nelle libertà, come il riconoscimento facciale, la profilazione dei movimenti di persone, il riconoscimento di targhe di veicoli o altro (cosiddetta *Smart Detection*), e ciò anche in tempo reale, ad alta risoluzione, con possibilità di registrazione audio e con elevato fattore d'ingrandimento delle immagini. Certo, lo Stato è chiamato a garantire la sicurezza interna della popolazione, nel suo insieme così come del singolo individuo, e la videosorveglianza vi contribuisce spesso in modo effettivo ed efficace. Molti casi di criminalità, anche gravi, hanno potuto essere risolti unicamente grazie alla videosorveglianza o a altri strumenti di controllo. La videosorveglianza è perciò diventata uno strumento potente per la lotta contro il crimine.

L'ordinamento giuridico svizzero assoggetta però la sorveglianza pubblica a limiti e condizioni, derivanti principalmente dai principi della proporzionalità e della legalità, nonché dalla garanzia delle libertà[3]. Tali

---

1 ANTONELLO SORO, La società sorvegliata – I nuovi confini della libertà, Roma 2016, pag. 4 (per contributi di altri autori nella stessa raccolta, si citerà in seguito: Convegno Roma 2016).

2 SORO, 2016, pag. 6-7.

3 ALEXANDER FLÜCKIGER/ANDREAS AUER, La vidéosurveillance dans l'œil de la Constitution, AJP/PJA Zurigo 2006 (8/2006), pag. 924 seg.

condizioni sono intese ad evitare che un dosaggio eccessivo delle misure di sicurezza possa compromettere il loro stesso scopo, vale a dire la garanzia di condizioni esterne favorevoli per l'esercizio di diritti e libertà del cittadino e per la realizzazione dello Stato democratico. Una certa limitazione dei diritti costituzionali è accettabile unicamente nella misura in cui siano rispettati i suddetti principi generali del diritto e sia dato un interesse pubblico preponderante legalmente previsto e garantito. In ogni caso, i diritti fondamentali rimangono intangibili nella loro essenza[4]. Pertanto, *«lo Stato deve attentamente valutare la compatibilità della videosorveglianza con i diritti e le libertà fondamentali»*[5], posto che nello Stato liberale è sempre la sicurezza a doversi misurare e giustificare nei confronti della libertà, non il contrario. Se questa valutazione non ha luogo correttamente, *«l'emergente rivoluzione tecnologica potrebbe condannare l'idea stessa di libertà individuale; (...) e, come un mito del passato, il pensiero liberale potrebbe perdere il suo privilegiato dominio nei nostri processi decisionali. (...)»*[6]. I sistemi di sorveglianza *«potrebbero essere pericolosi (...) poiché potrebbero dare origine a regimi di sorveglianza in cui tutti gli individui sarebbero costantemente controllati»;* nella peggiore delle ipotesi, la concentrazione di tutte le informazioni nelle mani di regimi autoritari potrebbe portare verso la *dittatura digitale (...)*[7]. L'uomo e le sue istituzioni statali sono, sì, curiosi per natura, ma questa curiosità può divenire malsana e condurre alle peggiori derive per delle intere società[8]. La videosorveglianza e le altre forme di monitoraggio elettronico di ampie parti di città, mosse da intenti a volte forse eccessivamente zelanti di sicurezza, possono essere il primo passo in questo senso e vanno perciò a loro volta accuratamente monitorate, disciplinate e regolarmente rivalutate nella loro proporzionalità.

---

4 Art. 36 della Costituzione federale della Confederazione svizzera (Cost.; RS 101).

5 RAINER J. SCHWEIZER, in Bernhard Ehrenzeller, Benjamin Schindler, Rainer J. Schweizer, Klaus A. Vallender, Die schweizerische Bundesverfassung, St. Galler Kommentar, terza edizione, Zurigo/San Gallo 2014, pag. 1224 n. 36.

6 YUVAL NOAH HARARI, 21 lezioni per il XXI secolo, Edizioni Bompiani Firenze – Milano 2019, pag. 80, 82, 100.

7 VINCENT MARTENET/JACQUES DUBEY, Commentaire Romand, Constitution fédérale, Préambule – art. 80 Cst., Basilea 2021, art. 13 Cost., pag. 494 n. 10; HARARI, 2019, pag. 104.

8 LUC GONIN, Droit constitutionnel suisse, Ginevra – Zurigo 2021, pag. 641 n. 2086.

Prima parte:
Principali misure e strumenti di sorveglianza e di controllo pubblico

1. Panoramica

La sorveglianza e il controllo pubblici si manifestano principalmente nei seguenti modi:
- monitoraggio a lungo termine del demanio pubblico;
- sorveglianza a breve termine di persone, del demanio o di beni pubblici in situazioni di pericolo per la sicurezza;
- monitoraggio e analisi di scene di incidente o di crimine;
- identificazione di targhe di veicoli;
- rilevamento di infrazioni al codice stradale[9].

2. Principali misure e strumenti[10]

2.1. Videosorveglianza

2.1.1. Scopi

La videosorveglianza pubblica è l'attività di vigilare su un luogo o un bene amministrativo pubblico a distanza, di norma a lungo termine, con apparecchi fissi o mobili in grado di raccogliere immagini e suoni e di trasmetterli a una centrale di sorveglianza, principalmente per stoccaggio a fini dissuasivo-repressivi (videosorveglianza dissuasiva) o, in determi-

[9] Si tratta di attività di controllo del rispetto di norme sulla circolazione stradale attuate in particolare tramite strumenti fotografici o di rilevamento della velocità di veicoli e perlopiù disciplinate dal diritto federale. Poiché il presente contributo mira a proporre delle modifiche legislative del diritto cantonale, tali attività di controllo non saranno oggetto di ulteriori approfondimenti in questa sede.

[10] Gli strumenti di sorveglianza aumentano regolarmente di numero (vedi, ad esempio, i droni dotati di videocamera, oppure i nuovi strumenti di pagamento dei parcheggi pubblici, i quali possono permettere, potenzialmente, l'allestimento di profili di movimento dei veicoli sulla base dei parcheggi utilizzati). Sia i droni che i nuovi strumenti di pagamento dei parcheggi pubblici non verranno tematizzati in questo contributo.

nate circostanze, per visione in tempo reale (videosorveglianza osservativa).

Grazie a un insieme di applicazioni tecnicamente molto performanti e con molteplici finalità, integrate ai sistemi di videosorveglianza pubblica standard, negli ultimi tempi la videosorveglianza è passata dal semplice presidio elettronico fisso grandangolare del demanio pubblico per la sorveglianza dissuasiva a tutela della sicurezza e dell'ordine pubblico e per la sorveglianza osservativa del traffico, al riconoscimento facciale e all'inseguimento e tracciamento (o profilazione) di movimenti e comportamenti, anche in tempo reale, di persone, sagome, colori o veicoli. Tecnicamente, i dati personali raccolti possono essere facilmente interfacciati con i dati elaborati in altre banche dati, creando così i presupposti per l'elaborazione di estesi profili della personalità. Le videocamere non sono perciò più unicamente monofunzionali, ma sono diventate multifunzionali, nel senso che possono essere adibite a diversi scopi e attività di sorveglianza, a seconda delle contingenze e necessità del momento. Così, una videocamera preposta alla sorveglianza dissuasiva o osservativa del demanio pubblico o del traffico può, in determinate circostanze, essere utilizzata in modalità invasiva, ad esempio per il riconoscimento facciale o di movimento.

2.1.2. Elaborazione di dati personali

Le immagini e i suoni ottenuti e registrati tramite videosorveglianza sono suscettibili di contenere dati personali ogniqualvolta si riferiscono a una o più persone identificate o identificabili. Tali dati possono essere di natura sensibile, nella misura in cui danno informazioni sulla salute, la sfera intima o l'appartenenza a un'etnia, o sulle opinioni politiche, sindacali o religiose. Il colore della pelle, lo stato generale di salute, i simboli politici, determinate pratiche o attitudini che rivelano l'appartenenza religiosa, politica, sindacale, l'orientamento sessuale o altro, sono degli elementi della persona che la videosorveglianza può rilevare. Se le immagini e i suoni sono registrati su supporto di dati, la videosorveglianza implica un'elaborazione di dati personali ai sensi della legislazione sulla protezione dei dati personali. Al contrario, se le persone non sono identificabili (ad esempio, se la risoluzione delle immagini è troppo debole, o

quando nessuna persona entra nel campo di visione della videocamera), non è data un'elaborazione di dati personali[11]. Anche la videosorveglianza senza registrazione di immagini o suoni non costituisce un'elaborazione di dati personali ai sensi della precipua legislazione. Da notare tuttavia che la possibilità di pilotare le videocamere e di seguire determinate persone, volti, sagome, colori o altro, ad alta risoluzione, con elevato fattore d'ingrandimento immagine e con possibilità di ascolto di suoni, può comportare una violazione dei diritti di personalità e delle libertà ai sensi della Costituzione, anche in assenza di registrazione delle immagini e dei suoni. Il criterio della registrazione delle immagini e dei suoni non è perciò assoluto per decidere dell'esistenza o meno di una violazione dei diritti costituzionali del cittadino e per definirne la gravità.

2.1.3. Principali strumenti e applicazioni di videosorveglianza

2.1.3.1. Videocamera per monitoraggio del demanio pubblico

Si tratta di un dispositivo elettronico utilizzato per registrare immagini e suoni su supporto di memorizzazione. Nel settore pubblico le videocamere sono posizionate in modo fisso nei diversi punti strategici per la sicurezza e l'ordine pubblico, creando così una rete di videosorveglianza di principio statica e controllabile a lunga distanza e da remoto, ma che può presentare una certa dinamicità, potendo essere ampliata, spostata o ridotta a seconda delle contingenze di sicurezza o di ordine pubblico del momento o degli spostamenti dei punti cruciali di criminalità.

2*.1.3.2. Videocamera mobile Bodycam per interventi in situazioni di pericolo per la sicurezza*

Le Bodycam sono videocamere che vengono portate all'uniforme dell'agente di polizia e attivate in situazioni pericolose per la sicurezza dell'agente stesso o delle persone coinvolte. Sono intese avere uno scopo dissuasivo o preventivo su una cerchia ristretta di persone o su di una singola persona pronta a fare uso della violenza, grazie a registrazioni di immagini e suoni che possono essere successivamente analizzate e utiliz-

[11] FLÜCKIGER/AUER, 2006, pag. 934.

zate come mezzi di prova. Anche lo stesso cittadino può avvalersene come prova per la valutazione del comportamento della polizia.

2.1.3.3. Applicazioni di riconoscimento facciale e di movimento

La videosorveglianza può essere tecnicamente integrata con applicazioni di riconoscimento facciale o di movimento. Il riconoscimento facciale costituisce una tecnica d'identificazione, rispettivamente di verifica di una persona a partire da una o più immagini che la ritraggono[12]. Si basa sull'analisi di caratteristiche visibili del volto date dal loro ordine geometrico e dalle caratteristiche della superficie della pelle. Presuppone una raccolta originaria di immagini del volto salvate in un formato particolare (Template) in una specifica banca dati e successivamente paragonate con le immagini riprese da una videocamera (verifica dell'immagine in tempo reale con il Template), ad esempio in un controllo degli accessi[13]. Come qualsiasi altro sistema di autenticazione biometrica, presentano un margine di errore (falsi positivi o falsi negativi), in particolare perché i volti invecchiano e si allontanano così dal volto di riferimento, oppure subiscono ferite o operazioni. In ambito di sicurezza pubblica, il riconoscimento facciale biometrico costituisce un nuovo strumento di ricerca e d'inchiesta di polizia basato sul paragone dei dati biometrici dei volti ripresi da videocamere appositamente predisposte a tale scopo con quelli presenti in banche dati di persone ricercate o scomparse. Alcune applicazioni di riconoscimento facciale possono essere programmate per riconoscere non soltanto il volto, ma anche particolari emozioni, espressioni o mimiche.

Il riconoscimento facciale può essere integrato con l'inseguimento e la profilazione dei movimenti della persona in questione, grazie all'incrocio dei risultati di riconoscimento facciale di più videocamere situate nello spazio pubblico[14]. L'inseguimento e la profilazione di movimento può

---

12 Sulla distinzione tra riconoscimento e verifica facciale, vedi MONIKA SIMMLER/GIULIA CANOVA, Gesichtserkennungstechnologie: Die «smarte» Polizeiarbeit auf dem rechtlichen Prüfstand, in: Sicherheit und Recht, Zurigo 2021, n. 3/2021, pag. 107.

13 GÜNTER KARJOT, Fähigkeiten der Gesichtserkennung, DIGMA, Zeitschrift für Datenrecht und Informationssicherheit, Zurigo 2019.1, pag. 6 seg.

14 SIMMLER/CANOVA, 2021, pag. 109.

essere programmato per seguire non soltanto dei volti, ma anche determinate sagome, colori o altro. La tecnica può essere impiegata, tra l'altro, come misura di sicurezza per la prevenzione e protezione da pericoli concreti, ad esempio nell'ambito di manifestazioni e eventi di massa, per il riconoscimento e fermo, rispettivamente allontanamento preventivo di persone schedate come pericolose (*Hooligans* e simili). Si tratta in tali casi di una sorveglianza concreta e mirata su uno o più individui pericolosi. Il riconoscimento facciale può essere impiegato anche a conferma di sospetti o indizi che da soli non sono sufficienti a giustificare l'apertura di inchieste preliminari penali o di polizia[15]. Può inoltre trovare applicazione nel perseguimento penale vero e proprio, e quindi successivamente alla commissione di un reato, per l'identificazione di persone in materiali videografici risultanti dalla videosorveglianza del demanio pubblico.

2.1.3.4. Videocamere per analisi di scene di incidente o di crimine

Con cosiddette telecamere *Dashcam total view* montate sui veicoli di polizia si possono ottenere, sia a veicolo fermo che in movimento, immagini e video a 360°, rendendo possibile in questo modo riprese complete e senza angoli ciechi, che possono essere utilizzate successivamente per l'analisi di una scena di incidente o di un crimine.

Le *Dashcam* possono, tecnicamente, essere impiegate anche per l'identificazione di targhe di veicoli i cui proprietari hanno debiti pregressi con le autorità di polizia (multe). Questo tipo di impiego è, come vedremo in seguito, giuridicamente problematico, poiché possono costituire una cosiddetta *Fishing Expedition* (vedi cap. 5).

2.1.4. Caratteristiche tecniche

A seconda dei modelli, le moderne tecnologie di videosorveglianza si distinguono attraverso una serie di caratteristiche, tra le quali, per quanto qui di rilievo:

- alta risoluzione, accuratezza e qualità d'immagine, anche in condizioni di scarsa luminosità;
- elevato fattore di ingrandimento immagine (zoom);

---

15 SIMMLER/CANOVA, 2021, pag. 110.

– registrazione audio;
– possibilità di roteazione del campo visivo in tutte le direzioni;
– rilevamenti termici.

2.1.5. Caratteristiche relative all'ubicazione

2.1.5.1. Videosorveglianza fissa

La videosorveglianza avviene in modo fisso quando è installata in modo stabile e saldo in una determinata postazione prescelta del demanio pubblico.

2.1.5.2. Videosorveglianza mobile

La videosorveglianza è mobile quando lo strumento impiegato è portatile, rispettivamente può essere trasferito a breve termine in specifici luoghi o situazioni che presentano una criticità momentanea per la sicurezza e l'ordine pubblico (ad esempio, *Bodycam* [vedi cap. 2.1.3.2] o altri apparecchi di sorveglianza movibili).

2.1.6. Caratteristiche temporali

La sorveglianza pubblica può essere attuata a lungo o a breve termine, a seconda delle condizioni e congiunture di sicurezza del momento.

2.1.6.1. Videosorveglianza a lungo termine

La videosorveglianza a lungo termine avviene a durata, di principio, indeterminata e risponde alla necessità di prevenire e contrastare fenomeni di criminalità diffusa. È finalizzata a garantire la sicurezza e l'ordine pubblico in aree urbane, in particolare a vantaggio delle zone maggiormente interessate da fenomeni di degrado, in condizioni di sicurezza ordinarie. È attuata di norma tramite una rete di videocamere a postazione fissa (vedi cap. 2.1.5.1), nelle modalità dissuasiva (vedi cap. 2.1.7.2) oppure osservativa del traffico (vedi cap. 2.1.7.3).

2.1.6.2. Videosorveglianza a breve termine

La videosorveglianza a breve termine è attuata su un periodo delimitato di tempo, in circostanze di criticità momentanea per la sicurezza e l'or-

dine pubblico. È finalizzata al mantenimento dell'ordine e della sicurezza in occasione di manifestazioni pubbliche oppure durante interventi di polizia, quando esiste un rischio oggettivo per l'incolumità delle persone e degli agenti di polizia coinvolti. Può essere attuata in modalità osservativa (vedi cap. 2.1.7.3), invasiva (vedi cap. 2.1.7.1), dissuasiva (vedi cap. 2.1.7.2), o in combinazione tra di esse, a seconda delle necessità del caso specifico. Per la videosorveglianza a breve termine possono, tecnicamente, essere impiegati strumenti di videosorveglianza mobile (vedi cap. 2.1.5.2), oppure può essere utilizzatala rete di videocamere fisse già presente sul territorio per la sorveglianza dissuasiva del demanio pubblico (vedi cap. 2.1.5.1).

2.1.7. Modalità di videosorveglianza

Le principali modalità di sorveglianza, tecnicamente combinabili tra di loro, sono le seguenti[16]:
- sorveglianza invasiva;
- sorveglianza dissuasiva;
- sorveglianza osservativa.

2.1.7.1. Videosorveglianza invasiva

Con videosorveglianza invasiva s'intende l'osservazione delle immagini in chiaro, a schermo, in tempo reale e continuato, indipendentemente dalla presenza di un pericolo o di una minaccia concreta, in circostanze specifiche e qualificate dal punto di vista della sicurezza. Può essere predisposta a sorvegliare un determinato individuo o gruppo di individui considerati pericolosi[17]. Avviene, a seconda del caso, con o senza registrazione delle immagini, ed è finalizzata al tempestivo riconoscimento di eventi illeciti o delittuosi concreti e all'intervento immediato delle forze dell'ordine. Può presentare anche un aspetto dissuasivo, se attuata al fine di prevenire degli illeciti da parte di persone ritenute pericolose.

---

16 Vedi anche DTF 136 I 87, consid. 8.2.1 e DTF 133 I 77, consid. 4.2.

17 JEAN RÜEGG, ALEXANDRE FLÜCKIGER, VALÉRIE NOVEMBER, FRANCISCO KLAUSER, Vidéosurveillance et risques dans l'espace à usage public: représentations des risques, régulation sociale et liberté de mouvement, Ginevra – Friborgo 2006, pag. 7.

Rientra nell'ambito del diritto penale, di polizia e di salvaguardia della sicurezza interna[18].

2.1.7.2. Videosorveglianza dissuasiva

Con la videosorveglianza dissuasiva (o preventiva e repressiva) s'intendono prevenire minacce e turbamenti alla sicurezza e all'ordine pubblico tramite la posa ben riconoscibile di apparecchi di videosorveglianza con un campo di visione circoscritto a uno specifico bene pubblico d'uso comune. La videosorveglianza dissuasiva è perciò utilizzata per incitare colui che potrebbe potenzialmente avere un'attitudine inadeguata a adottare il comportamento richiesto[19]. A differenza della sorveglianza invasiva, quella dissuasiva non è associata né a sospetti concreti, né alla sorveglianza di specifici eventi o di singole persone ritenute pericolose[20]. La videosorveglianza dissuasiva è, piuttosto, predisposta per la registrazione costante di segnali d'immagine (idealmente, con l'applicazione di filtri della privacy per la schermatura di beni tutelati), indipendentemente da un evento concreto di sicurezza. L'analisi delle immagini non avviene in tempo reale, ma successivamente alla commissione di un atto illecito. In questo senso, la videosorveglianza dissuasiva non garantisce in modo diretto la sicurezza e l'ordine pubblico[21]. In quanto metodo di messa in sicurezza di mezzi di prova di potenziali infrazioni, la videosorveglianza dissuasiva è anch'essa in stretto nesso con il perseguimento penale e presenta quindi una doppia natura: dissuasiva (scopo principale) e repressiva (identificazione e perseguimento penale).

2.1.7.3. Videosorveglianza osservativa

Con la videosorveglianza osservativa (o in tempo reale) s'intende garantire la supervisione e, se del caso, il ripristino, del corretto flusso del traffico di autoveicoli in seguito a disturbi, disfunzioni o pericoli (incidenti stradali, ingorghi, ecc.). In determinate circostanze, la videosorveglianza

---

18 FLÜCKIGER/AUER, 2006, pag. 924.

19 RÜEGG, FLÜCKIGER, NOVEMBER, KLAUSER, 2006, pag. 7.

20 SIMMLER/CANOVA, 2021, pag. 109.

21 DTF 133 I 77, consid. 5.1.

osservativa entra in considerazione anche per la sorveglianza in tempo reale di flussi o assembramenti di persone (ma non di singole persone), a supporto e ottimizzazione dell'attività di polizia in loco (concetto dell'occhio tecnico esteso), ad esempio in caso di grandi manifestazioni o eventi, oppure per il controllo, in tempo reale e senza registrazione delle immagini, degli accessi a immobili dell'amministrazione pubblica, del parastato o altro. La videosorveglianza osservativa avviene perlopiù in tempo reale, con immagini in chiaro, e senza registrazione delle immagini e può di conseguenza essere considerata come un semplice mezzo tecnico di osservazione, in sostituzione della presenza fisica in loco dell'agente di polizia[22]. Non è tuttavia esclusa a priori la registrazione delle immagini e quindi l'elaborazione di dati personali. Per questo tipo di videosorveglianza sono utilizzate, di norma, tecnologie, rispettivamente impostazioni video, che non consentono d'identificare singole persone o targhe di veicoli, ma che forniscono unicamente un'immagine panoramica. Tuttavia, le caratteristiche tecniche dei nuovi dispositivi di sorveglianza permettono già l'identificazione di targhe e di veicoli, e quindi dei loro proprietari, avvicinando la videosorveglianza osservativa a quella invasiva. Proprio tale mescolanza di modalità diverse di sorveglianza rende sempre più difficile una loro chiara distinzione, sia sul piano concettuale che operativo.

Come si vedrà in seguito, i tre tipi di videosorveglianza non sono soggetti allo stesso regime giuridico, in ragione del fatto che le loro finalità e il loro impatto e intrusività nei diritti delle persone sorvegliate non sono gli stessi. Le differenze sono dovute in particolare ai fattori seguenti[23]:

- *temporale*: a dipendenza della modalità di videosorveglianza, i dati e il comportamento registrati possono essere visionati e analizzati durante specifici periodi di conservazione delle immagini;
- *personale*: a dipendenza della registrazione delle immagini e dei suoni, i dati possono essere accessibili a più persone e possono essere comunicate a terzi;

22 FLÜCKIGER/AUER, 2006, pag. 924 segg.

23 FLÜCKIGER/AUER, 2006, pag. 925.

– *geografico*: a seconda dell'estensione della rete di sorveglianza e della presenza di applicazioni di tracciamento di movimenti o di riconoscimento facciale, i dati possono permettere il tracciamento e l'allestimento di un profilo più o meno esteso degli spostamenti di una singola persona;
– *tecnologico*: a seconda delle caratteristiche tecnologiche, la videosorveglianza può essere più o meno invasiva nei diritti della persona.

2.2. Strumenti di lettura e identificazione di targhe di veicoli

Nel caso di apparecchi di lettura e identificazione di targhe di veicoli mobili o stazionari, viene generato un set di dati con le lettere e i numeri della targa di controllo del veicolo ripreso da telecamere concepite, di principio, esclusivamente a tale scopo e questi dati vengono automaticamente confrontati con quelli presenti in banche dati di targhe di veicoli o di liste di veicoli ricercati o scomparsi (*Blacklist* di veicoli). Contrariamente alla raccolta di dati di controllo da parte di una pattuglia di polizia, il sistema consente la raccolta di dati in massa e praticamente illimitata, il che si traduce in un aumento significativo della sorveglianza da parte della polizia e dell'intensità di ricerca[24]. Il set di dati include, oltre al numero di targa del veicolo, anche l'ora, la posizione e la direzione del veicolo e, eventualmente, gli occupanti del veicolo[25].

La lettura di targhe automatizzata avviene tramite strumenti fissi (con tempistiche di uso, di principio, indeterminate) o mobili (di principio, a tempo determinato), i quali – in caso di rilevamento positivo – determinano la data, l'ora, il luogo, la direzione di marcia e il profilo di movimento del veicolo e danno avvio alla ricerca, all'identificazione e, se del caso, al fermo del veicolo e all'apertura della rispettiva inchiesta (identificazione del proprietario o detentore veicolo, eventualmente apertura di un procedimento amministrativo o penale, ecc.). La finalità della lettura e identificazione di targhe di veicoli consiste, come già sommariamente anticipato, nella ricerca e nel ritrovamento di veicoli scomparsi, rubati o

[24] STF 6B_908/2018, consid. 2.1.
[25] STF 6B_908/2018, consid. 3.2.

coinvolti in reati o che trasportano merci pericolose, oppure nel controllo del transito di veicoli su strade a traffico limitato, oppure ancora nel controllo dell'accesso a posteggi con barriera. La lettura e identificazione di targhe di veicoli rientra nella sorveglianza invasiva.

L'identificazione di targhe di veicoli può avvenire anche tramite sistema di lettura installato sull'autovettura di servizio della polizia (*Dashcam*). Il rispettivo software gestionale per la lettura e l'analisi delle targhe consente alla pattuglia, in tempo reale e direttamente su strada, durante il normale controllo dinamico del territorio, di consultare simultaneamente le informazioni contenute nelle banche dati connesse, elaborando le informazioni di ritorno. L'agente può controllare automaticamente tutti i veicoli che precedono o incrociano l'auto di servizio, tramite la rilevazione automatica delle targhe da parte delle telecamere, effettuando un controllo immediato tramite incrocio dei dati con altre banche dati. Il risultato viene poi elaborato dal sistema, fornendo alla pattuglia in tempo reale i risultati della consultazione e la banca dati di provenienza dell'informazione stessa e consentendo di fermare il veicolo nell'immediatezza per procedere agli atti di competenza (sulle criticità delle *Dashcam*, vedi cap. 6.4).

Seconda parte:
Interessi e valori giuridici in gioco

3. Sicurezza e ordine pubblico

3.1. Sicurezza

La sicurezza rappresenta una condizione ideale, mai pienamente raggiungibile, che lo Stato tende costantemente a conseguire[26]. La sicurezza – letteralmente, l'assenza di preoccupazione (dal latino: *sine cura*) – può essere definita come la consapevolezza che determinate contingenze esteriori non produrranno minacce, pericoli, conflittualità o danni. Il rag-

[26] MARKUS MOHLER, Grundzüge des Polizeirechts in der Schweiz, Basilea 2012, pag. 36 n. 88.

giungimento della consapevolezza di sicurezza crea una situazione o sensazione soggettiva di protezione e di rifugio ed è, fondamentalmente, conseguenza dell'istinto di tutela della vita e di sopravvivenza. Al contrario, se la consapevolezza della sicurezza non è data, lo stato di calma e di equilibrio con il mondo esteriore è alterato. Il sentimento d'insicurezza è, perciò, in relazione con determinate emozioni e percezioni soggettive e non generalizzabili del mondo esterno, fondamentalmente legate alla paura dell'ignoto, o anche all'odio per il crimine[27].

Giuridicamente, la sicurezza è un interesse protetto dallo Stato, il quale intende difendere l'individuo da situazioni, reali o presunte, di pericolo. Tutelati sono, da una parte, la popolazione nel suo insieme e la sua pace sociale, dall'altra gli interessi e i valori del singolo quali la vita, la salute, la libertà, la proprietà, dall'altra ancora le istituzioni e i beni pubblici. La sicurezza è, pertanto, tesa a garantire i diritti e le libertà fondamentali di ogni singolo individuo, nonché l'esistenza e la pace della collettività nel suo insieme. Sebbene si tratti di un interesse giuridico previsto e tutelato dalla Costituzione, la sicurezza è intesa come un dovere dello Stato e non come un diritto fondamentale del cittadino[28].

3.2. Ordine pubblico

L'ordine pubblico è terminologicamente più difficile da definire rispetto alla sicurezza pubblica, oltre a non essere separabile in modo chiaro da quest'ultima. La definizione più comune vuole che esso sia l'insieme di tutte le regole indispensabili, secondo una visione prevalente, per una convivenza ordinata tra i cittadini[29]. Costituisce un interesse di polizia da perseguire, se del caso, con delle limitazioni della libertà, a condizione che le stesse siano previste esplicitamente dal diritto e siano proporzionate. Come con la sicurezza, anche con l'ordine pubblico s'intende garantire condizioni tali affinché possano essere esercitati i diritti e le libertà individuali, nonché l'esistenza e la pace della collettività nel suo insieme.

---

27 RÜEGG, FLÜCKIGER, NOVEMBER, KLAUSER, 2006, pag. 19.

28 SCHWEIZER, 2014, pag. 1186 seg. n. 4, 9, 18, 35, 36, 37 e pag. 1216 n. 8.

29 MOHLER, 2012, pag. 38 n. 95 seg.

4. Libertà e diritti fondamentali

La sorveglianza pubblica mette in gioco diversi diritti e libertà fondamentali, tra cui la libertà di movimento (art. 10 cpv. 2 Cost.), il diritto d'essere protetto contro un impiego abusivo dei dati personali (diritto all'autodeterminazione informativa, art. 13 cpv. 2 Cost.), la libertà di riunione (art. 22 Cost.) e, in misura minore, il diritto al rispetto della sfera privata in pubblico (art. 13 cpv. 1 Cost.).

4.1. Libertà

Come si vedrà nel dettaglio al capitolo 5, quando lo Stato attua la videosorveglianza o un'altra forma di controllo pubblico, è la libertà individuale stessa a essere violata. Lo sviluppo tecnologico cui si assiste oggigiorno, le politiche di sorveglianza che spesso vi si orientano, molte volte senza adeguate analisi d'impatto sui diritti di libertà, impongono una rivisitazione del concetto di libertà individuale e un nuovo richiamo a questo valore cardine e fondante dello Stato di diritto.

Tutti gli esseri umani nascono liberi ed eguali in dignità e diritti[30]. È con questa solenne enunciazione che si apre la Dichiarazione universale dei diritti dell'uomo. Viene con ciò riconosciuto un ambito di autonomia individuale all'individuo – incomprimibile nel suo nucleo –, cui corrisponde il corollario obbligo di astensione d'interferenze arbitrarie da parte dello Stato. Lo Stato liberale mette la libertà umana al primo posto nella scala dei valori. Afferma, in definitiva, che tutta l'autorità si fonda sulla libera volontà degli individui, come espressione del loro sentire, dei loro desideri e delle loro scelte. La Dichiarazione universale dei diritti dell'uomo e le Costituzioni degli Stati democratici e di diritto declinano il concetto di libertà in varie forme, tra cui la libertà di movimento, di credo e di coscienza, d'opinione e d'informazione, d'espressione, la libertà artistica, di riunione e di associazione, la libertà economica, la libertà sindacale. Questi istituti strategici fondamentali degli ordinamenti costituzionali degli Stati moderni sono diretti a salvaguardare ai cittadini la

[30] Art. 1 della Dichiarazione universale dei diritti dell'uomo, Risoluzione 217A (III) dell'Assemblea Generale delle Nazioni Unite, 10 dicembre 1948.

possibilità di scelta nei principali dominii della loro esistenza, intesa come possibilità di realizzarsi liberamente, e sono stati iscritti negli ordinamenti fondamentali quale comprensione giuridica ultima sull'uomo. Anche la Costituzione svizzera protegge l'individuo nel compimento della libertà nelle sue varie forme e lo Stato è chiamato a partecipare all'attuazione del postulato costituzionale dell'uomo portatore di libertà. Deve perciò rispettare il diritto di ogni persona a non essere ostacolata nella libera realizzazione della propria vita, nella libera attuazione della stessa[31] e nella libera interazione con altre persone. Come verrà esposto al capitolo 4.2, la garanzia dello sviluppo e della realizzazione del progetto individuale di vita in libertà e in pace implica anche – e, oggigiorno, in modo particolare – il rispetto della riservatezza personale e dell'autodeterminazione informativa. Ciò significa che l'uomo ha il diritto di essere tutelato nelle sue caratteristiche più personali, in particolare attraverso la tutela dei suoi dati personali e la protezione contro il costante monitoraggio e documentazione da parte dello Stato.

Lo Stato moderno svizzero ha fatto del postulato dell'uomo portatore di libertà il suo stesso fondamento. Lo Stato si funzionalizza così alla massima tutela del singolo, secondo il principio generale che identifica nella persona umana libera il valore base e assoluto del sistema. La libertà come valore assoluto è anche presupposto e garanzia di democrazia, di pluralismo e vieta ogni discriminazione. Questa è la conquista dello Stato moderno, che si realizza nell'obbligo di rispettare e far rispettare la libertà da tutti, e di creare le basi istituzionali della società civile[32]. Lo Stato moderno non vi può rinunciare, le democrazie non possono rischiare di allontanarsi da questa loro identità profonda. Di più: è stato scritto che sui diritti e sulle libertà fondamentali non si può trattare[33]. Quando lo Stato monitora e controlla in qualche forma il cittadino, è questo valore fondamentale del cittadino che può essere violato.

---

31 SORO, 2016, pag. 3 seg.

32 In questo senso, vedi anche EVA MARIA BELSER/BERNHARD WALDMANN, Grundrechte I, Zurigo – Basilea – Ginevra 2021, pag. 18 n. 21 seg.

33 ARMANDO SPATARO, Convegno Roma 2016, pag. 28 seg.

4.2. Diritti alla riservatezza e alla protezione dei dati personali

Oltre ai diritti di libertà, all'individuo sono garantiti costituzionalmente i diritti della personalità, in particolare il diritto alla riservatezza (o diritto alla protezione della sfera privata, o diritto alla privacy) e i diritti della protezione dei dati personali, in particolare il diritto all'autodeterminazione informativa.

L'art. 13 cpv. 1 Cost.[34] garantisce, innanzitutto, il diritto al rispetto della sfera privata, attraverso la protezione dell'identità, della reputazione, delle relazioni sociali e dei comportamenti intimi di ogni persona fisica, vale a dire le manifestazioni di una persona che non sono accessibili al pubblico. In questo senso, il campo di applicazione dell'art. 13 Cost. è limitato negativamente dal criterio dell'accessibilità al pubblico: un determinato comportamento non rientra nel campo di protezione della norma costituzionale quando è pubblicamente riconoscibile e visibile e quando non esiste un interesse a mantenerlo segreto o confidenziale. Quando, invece, un tale interesse esiste, un determinato comportamento (ad esempio, le manifestazioni di pietà e dolore presso la tomba di un defunto) è protetto dalla garanzia costituzionale della vita privata, anche se è osservabile in pubblico[35]. In tal caso, emerge anche nell'area pubblica il diritto alla riservatezza, all'invisibilità, all'opacità, alla libertà dal controllo[36], al ritirarsi dal mondo[37], all'essere lasciato in pace nello svolgimento della propria vita, delle proprie relazioni sociali e della personalità nella propria sfera privata (*right to be let alone*)[38].

L'art. 13 cpv. 2 Cost. riconosce, dal canto suo, il diritto di ogni persona di essere protetta contro l'impiego abusivo dei propri dati personali. Così, la protezione dei dati contribuisce alla protezione dell'individuo dal

---

34 Vedi anche art. 8 cpv. 2 lett. d Costituzione cantonale del 14 dicembre 1997 (Cost./TI; RL 101.000) e art. 8 Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950 (Convenzione europea dei diritti dell'uomo; CEDU; RS 0.101)

35 FLÜCKIGER/AUER, 2006, pag. 932.

36 SORO, 2016, pag. 5.

37 VINCENT MARTENET/JACQUES DUBEY, 2021, pag. 493 n. 7.

38 WARREN/BRANDEIS, Harvard Law Review 1890; FLÜCKIGER/AUER, 2006, pag. 932.

pericolo di un esercizio illecito e sproporzionato del potere informativo. La protezione offerta dall'art. 13 cpv. 2 Cost. comporta, tra l'altro, il diritto della persona di essere informata sui dati che sono elaborati sul suo conto (diritto di accesso), così come il diritto di ottenerne la rettifica o l'eliminazione nel caso in cui siano inesatti, inutili o raccolti in modo illecito. L'art. 13 cpv. 2 Cost. è ulteriormente concretato dalle legislazioni federale e cantonali sulla protezione dei dati. Con il riconoscimento, da parte della dottrina e della giurisprudenza[39], del cosiddetto diritto all'autodeterminazione informativa, all'art. 13 cpv. 2 Cost. viene oggigiorno attribuita una portata più ampia rispetto al solo diritto di protezione contro l'impiego abusivo dei dati. Il diritto all'autodeterminazione informativa implica la facoltà – di principio – della persona stessa di poter determinare se e per quale scopo le informazioni raccolte sul suo conto – anche quelle accessibili al pubblico – possano essere elaborate.

Così, qualora la sorveglianza pubblica implichi l'elaborazione – vale a dire in particolare la raccolta, la conservazione e la trasmissione – di dati personali sotto forma di immagini o suoni, essa rientra nel campo di applicazione dell'art. 13 cpv. 2 Cost. e delle leggi sulla protezione dei dati, le quali svolgono, in definitiva e come sottolineato in precedenza, il compito di conservare lo Stato liberale e democratico quando le autorità elaborano dati a carattere personale[40]. Il potere informativo dello Stato esercitato tramite la sorveglianza pubblica viene, di conseguenza, limitato dalle condizioni poste dalla protezione dei dati personali e dai diritti ivi istituiti, vale a dire, come visto, dalla facoltà dell'individuo di potersi comportare secondo la sua natura, senza doversi sentire costantemente sorvegliato e documentato[41].

---

39 Vedi, tra l'altro, EVA MARIA BELSER/BERNHARD WALDMANN, Grundrechte II, Schulthess Zurigo – Basilea – Ginevra 2021, pag. 88 n. 93 seg.

40 LUC GONIN, 2021, pag. 641 n. 2087.

41 RÜEGG, FLÜCKIGER, NOVEMBER, KLAUSER, 2006, pag. 50; LUC GONIN, 2021, pag. 641 n. 2087.

Terza parte:
Criticità della sorveglianza pubblica

5. In generale

I diritti e le libertà fondamentali visti nei capitoli precedenti sono irrinunciabili e inalienabili in modo egualitario per tutti gli uomini, indipendentemente dall'origine, razza, sesso, età, lingua, posizione sociale, modo di vita, convinzioni religiose, filosofiche o politiche, e menomazioni fisiche, mentali o psichiche (art. 8 Cost.)[42]. Come già visto precedentemente, essi garantiscono lo sviluppo e la realizzazione del progetto individuale di vita in libertà e in pace[43]; lo Stato deve rispettare il diritto di ogni persona a non essere ostacolata nella libera realizzazione della propria vita[44] e nell'espressione dell'autodeterminazione individuale[45]. Deve riconoscere in particolare il diritto alla protezione della sfera privata e alla protezione dei dati personali quale condizione per il libero sviluppo dell'individuo[46].

Quando non sono garantiti i diritti alla riservatezza o alla protezione dei dati personali, l'individuo può dover rinunciare a realizzare determinate caratteristiche della propria personalità, oppure può sviluppare un sentimento di soggezione a un obbligo al conformismo, rispettivamente una latente pressione all'adattamento, all'addomesticamento[47]. Viene a mancare la libertà di essere pienamente come si è, senza condizioni e pressioni esterne. Può essere violata, perlomeno indirettamente, la stessa libertà di movimento[48]. Ciò vale anche in ambito di videosorveglianza e di

---

42 Vedi, tra l'altro, SCHWEIZER, 2014, n. 2, pag. 168.

43 PIERRE TSCHANNEN, Staatsrecht der Schweizerischen Eidgenossenschaft, Berna 2011, n. 2 pag. 99.

44 Vedi *supra* cap. 4.1.

45 FLÜCKIGER/AUER, 2006, pag. 932.

46 BELSER/WALDMANN, 2021, pag. 79 n. 81, 86.

47 LUCIEN MÜLLER, Videoüberwachung in öffentlich zugänglicher Räumen – insbesondere zur Verhütung und Ahndung von Straftaten, Zurigo/San Gallo 2011, pag. 1 seg.; RÜEGG, FLÜCKIGER, NOVEMBER, KLAUSER, 2006, pag. 8, 52.

48 SABRINA GHIELMINI, CHRISTINE KAUFMANN, CHARLOTTE POST, TINA BÜCHLER, MARA WEHRLI, MICHÈLE AMACKER, Grund- und Menschenrechte in einer digitalen

controllo pubblico. Infatti, *«[…] l'esercizio del potere diviene, nel sorvegliato, coscienza inquieta della propria visibilità […]; che è, essa stessa, limitazione della libertà; […] la videosorveglianza è capace di annullare ogni possibilità per l'individuo di costruirsi liberamente […];l'individuo non è, infatti, più del tutto libero di vivere, nella segretezza, la propria personalità; […]»*[49]. Altri autori parlano di una barriera psicologica incontestabile per le persone che, per diversi motivi, non vogliono essere filmate e, quindi, di un rischio per la libertà di movimento, della libertà di andare e venire in modo anonimo[50].

Lo Stato di diritto, che prescrive nel contempo sicurezza, libertà e privacy, mira a realizzare un individuo sia sicuro, sia libero, sia il più possibile opaco. La sorveglianza pubblica deve rientrare in questo equilibrio psico-sociologico ricercato dal diritto, deve cioè essere accettabile, rispettivamente deve essere umanamente sostenibile e deve di conseguenza essere adeguatamente dosata, affinché si stabilisca un rapporto ragionevole tra lo scopo perseguito (la sicurezza e l'ordine pubblico) e la restrizione dei diritti di libertà e di personalità che ne consegue. In caso contrario, l'equilibrio tra sicurezza, trasparenza e libertà viene meno e la società libera può essere compromessa. Il potere dell'individuo sulla propria vita, che è dato anche dall'autodeterminazione sui propri dati personali, rischia di passare nelle mani del controllore. Nella peggiore delle ipotesi, cioè in caso di instaurazione di una trasparenza completa, il cittadino si troverebbe in uno stato di pura sottomissione alla conoscenza, al controllo e al potere altrui.

La videosorveglianza e le altre forme di controllo pubblico possono violare i diritti di libertà e di protezione dei dati in modo più o meno importante, a seconda delle circostanze concrete del singolo caso, in particolare delle modalità di sorveglianza attuate (dissuasiva, invasiva o osservativa), delle tecnologie di riconoscimento impiegate, dell'estensione della rete di sorveglianza e del grado di inter-operabilità delle banche

Welt, Schweizerisches Kompetenzzentrum für Menschenrechte (SKMR), 2021, pag. 51.

49 SORO, pag. 3 seg.

50 FLÜCKIGER/AUER, 2006, pag. 932.

dati[51]. La moderna sorveglianza pubblica tende a vedere o a documentare idealmente tutto, in qualsiasi momento. Ovviamente, la sorveglianza pubblica non viene, di norma, abusata per sorvegliare indiscriminatamente il cittadino (le autorità non ne avrebbero nemmeno le risorse), ma per la prevenzione e la repressione del crimine. Tuttavia, gli abusi – ad esempio, la videosorveglianza invasiva nell'ambito del monitoraggio standard del demanio pubblico, oppure la *Fishing expedition* – esistono e, in tali casi, la sorveglianza diventa uno strumento arbitrario di potere che può ledere in modo significativo i valori fondamentali del cittadino[52]. Con *Fishing expedition* s'intende l'analisi di registrazioni di dati alla ricerca di possibili reati, in assenza di un sospetto concreto, rispettivamente la raccolta preventiva di dati, senza che vi sia un chiaro e concreto scopo di elaborazione.

Il grado di libertà concesso al cittadino è inversamente proporzionale al grado di pervasività della sorveglianza. Così, a seconda del «dosaggio» e della pervasività della sorveglianza, visibilità e controllo possono prevalere su diritti e libertà. Purtroppo, le odierne paure innescate dalla minaccia del terrorismo, ma anche dal crimine in generale, nonché da una certa tendenza al perfezionismo per l'ordine pubblico, rendono il cittadino sempre più disponibile a ampie concessioni riguardo alla propria libertà e alla protezione dei propri dati personali, in nome dell'interesse alla sicurezza e all'ordine pubblico. Di fronte in particolare al terrorismo, ma anche contro il crimine in generale, si usano sempre più spesso scorciatoie emergenziali come la sorveglianza a tappeto della società, a volte anche senza sufficiente trasparenza. Le autorità preposte alla sicurezza possono anche tendere a seguire e implementare scrupolosamente tutte le potenzialità tecniche offerte dalle nuove tecnologie, quasi fossero queste ultime e le rispettive aziende produttrici a definire (o, piuttosto, a eliminare?) i limiti della sorveglianza. Così, gli atti di inciviltà e il sentimento d'insicurezza finiscono per essere strumentalizzati da venditori di tecnologie di sorveglianza a fini commerciali, senza che l'autorità colga sempre pienamente questo fine. Anche le istituzioni e la politica possono

[51] STF 6B_908/2018, consid 3.2; FLÜCKIGER/AUER, 2006, pag. 933.

[52] DTF 136 I 87, consid. 8.1.

fare dell'insicurezza di una parte della società il loro cavallo di battaglia. Delle politiche dette di tolleranza zero sono, così, state elaborate in risposta a luoghi qualificati di zone di non-diritto, di fuori legge, l'idea essendo di non tollerare più nessuna violazione, anche soltanto potenziale o ipotetica, delle norme di sicurezza e di ordine pubblico[53]. Non si deve, però, permettere che il crimine determini un arretramento della garanzia dei diritti di libertà. Nella determinazione dei limiti del compito di sorveglianza, lo Stato e la società devono preliminarmente chiedersi a quanta libertà siano ancora disposti a rinunciare[54] e, soprattutto, devono operare maggiormente e con più efficacia nella prevenzione. Proprio in merito alla prevenzione, i recenti fatti di cronaca criminale in Ticino hanno rilanciato nei media la discussione sulla necessità di centri educativi chiusi per minorenni in difficoltà e con tendenze criminali, per fermarli prima che si mettano seriamente nei guai[55]. La sola sorveglianza è una capitolazione di fronte al crimine e anche un fallimento di chi è preposto all'educazione: *in primis* famiglia, autorità scolastiche e ecclesiastiche e media.

Oltre a ciò, la videosorveglianza può sollevare criticità anche dal punto di vista del principio della legalità[56]. Il deficit legislativo ha come conseguenza la sottrazione della sorveglianza pubblica al dibattito democratico. Per predisporre una videosorveglianza sostenibile dal punto di vista democratico non è, però, sufficiente una decisione delle autorità, ma è necessario che i rischi per la sicurezza che ne giustificano il ricorso siano precedentemente identificati e ponderati dal Legislatore prima di essere convertiti in un'automatizzazione della sorveglianza[57].

---

53 RÜEGG, FLÜCKIGER, NOVEMBER, KLAUSER, 2006, pag. 23.

54 SORO, 2016, pag. 3 seg.; LICIA CALIFANO, Convegno Roma 2016, pag. 147 seg. AUGUSTA IANNINI, Convegno Roma 2016, pag. 13 seg.

55 RETO MEDICI, Sfide tra bande in tempo reale, La Domenica Corriere del Ticino, 12 dicembre 2021.

56 DTF 136 I 87 Consid. 8.3.

57 RÜEGG, FLÜCKIGER, NOVEMBER, KLAUSER, 2006, pag. 15.

6. Riguardo ad alcuni nuovi strumenti e applicazioni di sorveglianza pubblica

6.1. Bodycam

Ammesso che l'uso delle Bodycam possa, almeno in singoli casi, avere un effetto dissuasivo sulla commissione di atti reprensibili, il loro impiego può implicare anche delle violazioni dei diritti quali il diritto all'immagine, il diritto d'espressione e il diritto all'autodeterminazione informativa quali espressioni dei diritti di personalità delle persone direttamente interessate dalla registrazione, ma anche di terze persone non direttamente coinvolte nei fatti. La violazione si realizza attraverso una restrizione dei diritti dovuta alla consapevolezza di una registrazione d'immagini e di suoni in un contesto particolarmente delicato e importante per il loro esercizio. La violazione dei diritti del cittadino può risultare accresciuta se, successivamente alla raccolta, i dati – che possono essere meritevoli di particolare protezione ai sensi dell'art. 4 cpv. 2 della Legge sulla protezione dei dati personali[58] a ragione del contesto, potenzialmente penale, in cui vengono raccolti – sono interfacciati con altre banche dati, i cui scopi sono diversi da quelli per i quali i dati sono stati originariamente raccolti. A differenza della videosorveglianza di un intero comparto del demanio pubblico, dove la sensazione di sorveglianza può essere soggettivamente più ridotta, la sensazione di sorveglianza e di documentazione dell'agire delle persone interessate dalle riprese di una Bodycam può quindi essere più importante. A causa di un certo effetto inibitorio delle libertà di espressione e di movimento e del diritto alla propria immagine e all'autodeterminazione informativa, la videosorveglianza mobile tramite Bodycam – benché, di principio, di natura dissuasiva – rappresenta una forma di controllo del cittadino di una certa invasività.

6.2. Riconoscimento facciale

Il riconoscimento facciale – in quale rappresenta una forma di riconoscimento biometrico – implica un elevato potenziale di violazione dei di-

[58] Legge sulla protezione dei dati personali del 9 marzo 1987 (LPDP; RL 163.100).

ritti e delle libertà fondamentali (*in primis*, la libertà di movimento e il diritto all'autodeterminazione informativa), per l'ampia discrezionalità e possibilità di utilizzo potenzialmente illimitate che implica, e quindi in particolare per il rischio di passaggio dalla sorveglianza mirata di alcuni individui alla sorveglianza indiscriminata, o di massa, ad esempio di persone presenti a manifestazioni politiche o sociali che non sono altrimenti oggetto di sorveglianza particolare da parte delle forze dell'ordine e per la possibilità di interconnessione dei dati raccolti con altre banche dati[59]. La tecnologia viene usata in taluni altri Paesi anche per l'identificazione di persone che circolano sui mezzi pubblici senza titolo di trasporto valido. In altri se ne valuta l'impiego per la gestione della pandemia da COVID: chi non si tiene alle distanze minime o non porta la mascherina, riceve un messaggio (SMS) di avviso o una multa.

Spesso il riconoscimento facciale trova, anche in Svizzera, rapido e acritico impiego, soprattutto nel settore della polizia, senza una precedente, sufficiente discussione giuridica in particolare sull'efficienza, trasparenza, legalità e costituzionalità[60]. Il riconoscimento facciale presuppone, però, e come si vedrà nei seguenti capitoli, delle basi legali di rango formale, costituendo i dati biometrici dei dati meritevoli di particolare protezione elaborati in modo sistematico. Tali basi legali non sono, oggigiorno, previste né nel diritto cantonale nell'ambito dell'attività preventiva di polizia, né in quella più prettamente repressiva disciplinata dal diritto processuale penale svizzero[61] e non può quindi essere attuato. Se invece, nella pratica, dovesse già avvenire, andrebbe interrotto e sostituito da test pilota per la valutazione dell'idoneità e necessità. Andrebbe poi effettuata un'accurata analisi d'impatto sui diritti e andrebbe infine, se del caso, disciplinato, nei suoi limiti e nelle sue condizioni, dal Legislatore[62].

---

59 SIMMLER/CANOVA, 2021, pag. 112.

60 SIMMLER/CANOVA, 2021, pag. 106 seg., 112 seg.

61 SIMMLER/CANOVA, 2021, pag. 114 seg.

62 BEAT RUDIN/LIVIA MATTER, Gesichtserkennung auf dem Vormarsch, DIGMA Zeitschrift für Datenrecht und Informationssicherheit, Zurigo 2019, pag. 4 seg., 14 seg. Delle iniziative popolari a livello europeo (ad esempio, «Reclaim your Face») e svizzero (gesichtserkennung-stoppen.ch di AlgorithmWatch, Amnesty Schweiz e Digi-

6.3. Strumenti di riconoscimento di targhe di veicoli

Il riconoscimento di targhe rappresenta una misura di identificazione e riguarda sia il diritto alla libertà personale, sia il diritto alla privacy. La raccolta di dati rientra sostanzialmente nell'ambito di un controllo d'identità convenzionale, che di per sé non costituisce una grave ingerenza nel diritto alla libertà personale (art. 10 cpv. 2 Cost.) e nell'autodeterminazione informativa (art. 13 cpv. 2 Cost.). Tuttavia, gli apparecchi di identificazione di targhe di veicoli non si limitano alla semplice raccolta e conservazione delle informazioni di identificazione. Piuttosto, i dati raccolti possono essere incrociati con altre raccolte di dati e confrontati automaticamente. Gli apparecchi di identificazione di targhe di veicoli consentono perciò l'elaborazione seriale e simultanea di insiemi di dati complessi e di grandi dimensioni in frazioni di secondo, che va oltre la raccolta di informazioni sul traffico convenzionale e i sistemi di ricerca in ambito di sicurezza. La combinazione con altri dati raccolti può costituire la base per profili di personalità o di movimento. L'interferenza con i diritti fondamentali, che non è né specifica dell'evento né basata su uno specifico sospetto, può avere, da un lato, un effetto dissuasivo, dall'altro, può influenzare la libertà di movimento, per la consapevolezza della possibilità di un uso (segreto) successivo da parte delle autorità e la sensazione di sorveglianza associata che ne risulta. Recentemente, il Tribunale federale ha valutato l'intromissione nei diritti e nelle libertà costituzionali che gli apparecchi d'identificazione automatica delle targhe di veicoli comportano, giudicandola importante a causa, appunto, della multifunzionalità e inter-connettività di questi strumenti con altre banche dati. In ogni caso, il Tribunale federale ha riconosciuto la necessità di disciplinare l'impiego di tali strumenti nel diritto formale[63].

tale Gesellschaft, lanciata il 18 novembre 2021) spingono, tuttavia, per una proibizione della sorveglianza biometrica di massa.

63 STF 6B_908/2018, consid. 2.1, 3.1, 3.2. In seguito a questa sentenza, il Dipartimento federale di Giustizia e Polizia ha deciso di rinunciare alla revisione dell'Ordinanza dipartimentale federale sugli strumenti di misurazione della velocità, di cui il Canton Ginevra aveva chiesto l'estensione del campo di applicazione agli strumenti d'identificazione automatica delle targhe di controllo, considerando l'Ordinanza in questione una base legale insufficiente.

6.4. Dashcam per il riconoscimento di veicoli i cui detentori hanno debiti pregressi con le autorità di polizia

L'uso di videocamere *Dashcam* installate su veicoli di polizia per la scansione sistematica e indiscriminata di targhe di veicoli per la ricerca di potenziali debitori di multe o altri debiti pregressi con le autorità di polizia rientra nella definizione di *Fishing expedition* (vedi cap. 5) ed è contraria ai principi della protezione dei dati, in particolare del principio della proporzionalità e della finalità.

Quarta parte: Condizioni legali e costituzionali della videosorveglianza e delle altre forme di controllo pubblico

Come visto nei capitoli precedenti, la videosorveglianza e il controllo pubblici possono ledere diritti e libertà fondamentali; la Costituzione federale (art. 36) e quella cantonale (art. 8) pongono le condizioni per la loro restrizione.

7.1. Base legale

La base legale prescritta dagli art. 36 cpv. 1 Cost. e 8 cpv. 3 Cost./TI quale fondamento di una restrizione lecita dei diritti fondamentali è la concretizzazione del principio della legalità (art. 5 cpv. 1 Cost.)[64]. Il principio della legalità comanda che ogni attività statale abbia il suo fondamento nella legge. La sua finalità principale è il rispetto della separazione dei poteri, dell'uguaglianza di trattamento e della proibizione dell'arbitrario, così come della garanzia della valutazione e dell'ancoraggio degli atti dello Stato da parte del popolo, rispettivamente dei suoi rappresentanti. Se la validità del principio della legalità si estende all'insieme degli atti imputabili allo Stato, le sue esigenze variano a seconda di diversi criteri, tra i quali conviene citare, in particolare, l'impatto delle misure sui diritti e gli obblighi dei cittadini[65]. Il Tribunale federale ha più

64 Vedi, in particolare, BELSER/WALDMANN, Grundrechte I, 2021, pag. 170 n. 24 seg.

65 FLÜCKIGER/AUER, 2006, cap. 2.4.

volte avuto l'occasione di sottolineare l'importanza del principio della legalità: in primo luogo, esso adempie a funzioni delle Stato di diritto, nel senso che con tale principio deve essere garantita al cittadino la riconoscibilità delle norme applicabili ad una determinata fattispecie e le conseguenze legali di un determinato comportamento[66]. Il TF ha affermato la necessità di basi legali esplicite riguardo a singoli tipi di elaborazione sistematica di dati personali, come la videosorveglianza del demanio pubblico[67]. Seguendo questa giurisprudenza, un rischio d'ingerenza illecita nella personalità è dato in particolare dall'assenza di trasparenza legale per quanto riguarda un determinato scopo e metodo di elaborazione di dati personali. Le basi legali dell'elaborazione di dati personali devono essere chiare e limitative dell'uso e devono evitare che quest'ultimo sia troppo discrezionale. Le esigenze di rango e di densità normativa da porre alla base legale sono tanto più elevate quanto più grave è l'ingerenza nei diritti fondamentali del cittadino e quindi quanto più elevato è il rischio di una loro lesione[68]. I fattori che determinano la gravità dell'ingerenza sono certamente la natura e la sensibilità dei dati, ma non solo: devono essere considerati anche lo scopo e il contesto della loro elaborazione, il volume dei dati trattati e la durata della loro conservazione, l'ampiezza della cerchia delle persone e autorità interessate, l'ambito giuridico concreto come pure il tipo di sistema, aperto (e in che misura) o chiuso, di raccolta e gestione dei dati. Se i dati sono meritevoli di particolare protezione (come è il caso nella videosorveglianza: si pensi ad esempio ai dati riguardanti lo stato di salute o l'appartenenza a un'etnia, a una religione), la base legale deve essere di rango formale[69].

La LPDP ha ripreso e concretato il principio della legalità per le elaborazioni di dati personali. Secondo l'art. 6 cpv. 1 LPDP, la base legale è necessaria quando i dati sono elaborati in modo sistematico, vale a dire con regolarità o durata (art. 4 cpv. 4 LPDP), come è il caso delle elaborazioni

66 DTF 109 Ia 273, consid. 4d.

67 STF 1C_315/2009; più in generale, sulla necessità di basi legali in caso di violazioni di diritti fondamentali, vedi DTF 126 I 50.

68 Vedi, tra l'altro, BELSER/WALDMANN, Grundrechte I, 2021, pag. 174 n. 29 seg.

69 Vedi in particolare FLÜCKIGER/AUER, 2006, pag. 926 seg.

di dati effettuate tramite la videosorveglianza o altri strumenti di controllo pubblico che registrano dati personali[70].

Gli altri motivi giustificativi dell'elaborazione di dati personali previsti dalla LPDP – la necessità per l'adempimento di compiti legali o il consenso delle persone interessate – possono giustificare unicamente elaborazioni di dati nel singolo caso, siano essi standard o meritevoli di particolare protezione (art. 6 cpv. 2 LPDP) e non possono perciò entrare in considerazione per la videosorveglianza o le altre forme di controllo pubblico qui in discussione, perlomeno non quando esse avvengono in modo sistematico[71].

7.2. Interesse pubblico e proporzionalità

La restrizione di diritti fondamentali deve innanzitutto essere giustificata da un interesse pubblico (art. 36 cpv. 2 Cost. e 8 cpv. 3 Cost./TI), che per quanto riguarda la videosorveglianza e le altre forme di controllo pubblico, sono la sicurezza e l'ordine pubblico (vedi anche cap. 3). Dal canto suo, il principio della proporzionalità (art. 36 cpv. 3 Cost. e 8 cpv. 3 Cost./TI) è centrale nel discorso della limitazione dei diritti e delle libertà fondamentali[72]. In quanto regola del buon senso fondamentale per la comprensione dello Stato di diritto e della giustizia, esso è determinante per l'insieme dell'elaborazione dei dati e per i suoi effetti sulla personalità, segnatamente per le categorie di dati elaborati, la tipologia e il metodo dell'elaborazione, la cerchia di persone interessate, il demanio pubblico interessato, la cerchia di persone aventi diritto d'accesso, la durata dell'elaborazione, la durata di conservazione dei dati e le misure di sicurezza. Lo scopo stesso dell'elaborazione – vale dire l'interesse pubblico

---

70 Si veda, a questo proposito, in particolare Messaggio n. 7061 del Consiglio di Stato del Canton Ticino del 18 marzo 2015 concernente la modifica della Legge cantonale sulla protezione dei dati personali del 9 marzo 1987 (LPDP) riguardante i motivi giustificativi e i principi che reggono l'elaborazione di dati personali (art. 6 e 7 LPDP).

71 In ogni caso, il fatto di percorrere una strada in modo riconoscibile e identificabile e di entrare così nel campo di visione di una videocamera di sorveglianza non implica automaticamente il consenso (implicito) all'elaborazione di dati, tanto più che un simile consenso rischierebbe di essere forzato e quindi di non rientrare nella definizione di libera manifestazione di volontà. Vedi, in proposito, FLÜCKIGER/AUER, 2006, pag. 927.

72 Vedi SCHWEIZER, 2014, pag. 1199, n. 41 seg.

perseguito – deve essere proporzionato. Secondo il principio della proporzionalità, ogni singolo elemento e fase dell'elaborazione, dalla raccolta dei dati, alle categorie di dati elaborati, alla loro durata di conservazione, deve essere idoneo e necessario al rispettivo scopo e deve sussistere un rapporto ragionevole di grandezza tra tale scopo e la restrizione della personalità che ne risulta. Nel suo insieme, l'elaborazione di dati deve costituire un ordine commisurato, appropriato, logico, adeguato, armonioso, ragionevole. Il principio di proporzionalità non tollera che una categoria d'interessi in gioco prevalga in modo smisurato, o disarmonico, rispetto agli interessi che vi si contrappongono. Maggiore è la restrizione della personalità – e ciò è, di principio, sempre il caso con la videosorveglianza e il controllo pubblico –, più pressante e urgente deve essere il bisogno sociale di sicurezza alla sua base (concetto di armonia e commisurazione degli interessi in gioco). Non è, quindi, sufficiente giustificare la videosorveglianza o un'altra forma di controllo pubblico unicamente invocando, in modo generale, la garanzia della sicurezza e dell'ordine pubblico[73], oppure richiamando, da parte dell'autorità competente, un (peraltro, soggettivo e scientificamente ancora da dimostrare) aumento della sensazione di sicurezza grazie alla videosorveglianza, così come non è sufficiente invocare i risultati repressivi della videosorveglianza o la riduzione dei costi per il mantenimento della sicurezza. Non basta, quindi, che la videosorveglianza sia adeguata allo scopo.

Poiché il diritto, e con esso il principio della proporzionalità, intende generare armonia, equilibrio, e più precisamente armonia psico-sociologica (essendo il fondamento del diritto di natura sociale e interpersonale), la videosorveglianza deve essere umanamente accettabile per il cittadino, sia dal punto di vista dello scopo perseguito, sia da quello dei mezzi utilizzati e della restrizione della personalità che ne risulta. Non appare, ad esempio, armonioso, e quindi umanamente sostenibile, che la videosorveglianza sia giustificata, come ribadito sopra, da un generico motivo di sicurezza e ordine pubblico. Un rischio generale e astratto non è, perciò, sufficiente e, sebbene non sia necessario che sussista un pericolo concreto, è perlomeno necessario che sia data una situazione di pericolo og-

[73] DTF 136 I 87, consid. 8.3; vedi *supra* cap. 3.

gettivamente motivabile, ad esempio un punto cruciale di criminalità. Non rientra, ad esempio, in tali fattispecie la videosorveglianza di determinati gruppi di persone al solo fine di sorvegliarle o emarginarle in qualche maniera, senza che sia dato un punto cruciale di criminalità. Sempre secondo il principio della proporzionalità, la videosorveglianza va riservata alla prevenzione e al perseguimento di reati più gravi, ad esclusione delle semplici contravvenzioni di ordine amministrativo. In questo senso, la videosorveglianza o gli strumenti d'identificazione di targhe di veicoli, tesi al controllo dell'osservanza di regole comportamentali minori (ad esempio, il divieto di *littering*, il divieto di passaggio del traffico su una determinata strada comunale), è critica dal punto di vista della giustificazione, rispettivamente della proporzionalità, tanto più che una tale sorveglianza può presentare il potenziale rischio di monitoraggio onnipresente del demanio pubblico. Pure sproporzionata è la videosorveglianza costante in modalità invasiva del demanio pubblico. Ad essa va favorita la videosorveglianza dissuasiva, che prevede l'analisi delle videoregistrazioni unicamente in seguito a una denuncia o requisitoria, oppure, eccezionalmente, quando non è altrimenti possibile ricostruire eventi delittuosi. Sproporzionata è, anche, la sorveglianza pubblica i cui scopi possono essere pienamente raggiunti anche con l'ausilio di misure meno incisive nei diritti delle persone, ma altrettanto efficaci dal punto di vista della sicurezza. Sproporzionata è, poi, la *Fishing Expedition* (vedi cap. 5). La sorveglianza pubblica deve essere proporzionata anche da un punto di vista temporale. Così, ad esempio, la videosorveglianza diurna di una piazza o di un giardino pubblico non si giustifica, di principio, se i problemi di sicurezza si presentano unicamente in orario notturno. Non è necessaria neppure la videosorveglianza durante tutto l'anno di una piazza o via, se i concreti problemi di sicurezza si pongono unicamente in determinate occasioni o eventi. Stesso discorso, di principio, per la portata territoriale della videosorveglianza: quest'ultima deve essere definita e delimitata al perimetro di bene pubblico di uso comune effettivamente interessato da problematiche di sicurezza e altri beni tutelati vanno schermati con filtri della privacy[74]. Sem-

[74] Il perimetro interessato va inteso anche dinamicamente, nel senso che può spostarsi col tempo, sia per contingenze sociali mutevoli, sia per lo spostamento di, rispettivamente allontanamento da, un centro cruciale per la sicurezza dovuto proprio alla

pre in attuazione del principio di necessità, gli impianti di videosorveglianza o di altre forme di controllo pubblico ed i programmi informatici ivi correlati vanno configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere raggiunte mediante dati anonimi o opportune modalità che permettano di identificare l'interessato solo in caso di necessità (ad esempio, tramite *Privacy Filters*). Così, in attuazione del principio di proporzionalità, rispettivamente dei criteri di pertinenza e non eccedenza, gli impianti di sorveglianza pubblica vanno configurati in modo da raccogliere esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese ed evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti. Il principio della proporzionalità si applica anche alla cerchia di personale abilitato alla videosorveglianza, che va limitato al minimo necessario, al fine di ridurre i rischi per la sicurezza dei dati o per il loro abuso, nonché disciplinato da regole sui diritti di accesso.

In definitiva, secondo il principio della proporzionalità, va attentamente valutata l'idoneità e la necessità di ogni misura di sorveglianza pubblica, tenendo conto delle circostanze concrete e adottando, se del caso, il tipo di sorveglianza – dissuasiva, osservativa, invasiva o mista – più consono alle reali necessità. In ogni caso, la sorveglianza pubblica deve essere sussidiaria rispetto ad altre misure, altrettanto efficaci ma meno incisive nei diritti delle persone interessate[75]. Poiché i rischi per la sicurezza e l'ordine pubblico possono variare nel tempo, ogni misura di sorveglianza va periodicamente rivalutata nella sua proporzionalità.

presenza di videocamere. Per quanto riguarda i filtri della Privacy (*Privacy Filters*), si tratta di Software che permettono il mascheramento delle sagome o dei volti delle persone tramite criptaggio delle immagini (*Scrambling*). I *Privacy Filters* sono di particolare importanza in ambito di videosorveglianza, poiché essa può implicare la raccolta di potenziali prove a monte di un reato o sospetto di reato e toccare una cerchia indeterminata di persone, di principio innocenti o non sospettate. L'anonimizzazione ottenuta tramite *Privacy Filters* può essere successivamente invalidata in caso di commissione di reato, per l'identificazione dei responsabili.

75 DTF 136 I 87, consid. 8.3.

7.3. Intangibilità del nucleo dei diritti fondamentali

I diritti fondamentali sono intangibili nel loro nucleo (art. 36 cpv. 4 Cost. e 8 cpv. 3 Cost./TI). Il nucleo di ogni diritto fondamentale non si lascia definire in modo astratto, ma deve essere determinato singolarmente per ogni diritto[76]. La restrizione del nucleo dei diritti di libertà e di protezione dei dati non si lascia giustificare e non è mai conforme alla Costituzione[77]. Nella sorveglianza pubblica potrebbe configurarsi una violazione del diritto all'autodeterminazione informativa, qualora dovessero essere introdotte strutture di sorveglianza talmente ampie che il cittadino non potrebbe più sottrarsi alla sorveglianza e alla registrazione statale su suolo pubblico. Lo stesso dicasi dell'introduzione di sistemi di videosorveglianza intelligenti e la sincronizzazione sistematica di banche dati, nella misura in cui tali misure non dovessero più essere compatibili nemmeno con la dignità umana[78].

7.4. Principio della finalità

Il principio della finalità implica che i dati personali raccolti non vengano utilizzati o trasmessi per uno scopo che, secondo la buona fede, sarebbe incompatibile con quello per il quale originariamente erano stati raccolti (vedi in particolare art. 7 cpv. 4 LPDP). Protetta è la fiducia del cittadino nello scopo dell'elaborazione legalmente previsto o deducibile dalle circostanze concrete secondo il principio della buona fede. Nel discorso sulla videosorveglianza e le altre forme di controllo pubblico, ciò significa che le immagini non possono essere abusate, ad esempio, a fini voyeuristici o di *Fishing Expedition* (vedi cap. 5).

---

76 DTF 143 I 292, consid. 2.4.1. MARKUS SCHEFER, in Die Kerngehalte von Grundrechten – Geltung, Dogmatik, inhaltliche Ausgestaltung, Berna 2001, pag. 448, indica, in merito alla libertà personale, che il nucleo del diritto all'autodeterminazione individuale garantito dall'art. 10 Cost. non si lascia descrivere in modo generale. Il pericolo di una violazione del nucleo aumenta con l'intimità o la vicinanza alla personalità del comportamento di una persona, di cui lo Stato prende conoscenza.

77 BELSER/WALDMANN, Grundrechte I, 2021, pag. 168, n. 22.

78 MÜLLER, 2011, pag. 134.

7.5. Principio della buona fede (o della trasparenza)

Questo principio, previsto nel diritto ticinese della protezione dei dati dall'art. art. 7 cpv. 2 LPDP, comporta che in ogni caso sia adeguatamente garantita l'informazione delle persone interessate quanto alla sorveglianza pubblica, ad esempio, per quanto riguarda la videosorveglianza, tramite cartelli indicanti chiaramente perlomeno la presenza dell'impianto e l'organo responsabile. Secondo il Tribunale federale, la violazione del principio della finalità implica una violazione qualificata dei diritti fondamentali[79], motivo per cui v'è necessità di informazioni trasparenti che rendano pienamente edotti gli utenti[80], idealmente con un cartello ad ogni videocamera. Rimangono riservate modalità e tempistiche d'informazione diverse, allorquando la stessa potrebbe compromettere l'esito di inchieste penali.

7.6. Principio della liceità

Il principio della liceità (art. 7 cpv. 1 LPDP) impone allo Stato in particolare di esaminare la conformità delle sue elaborazioni di dati con l'insieme del diritto, e non soltanto con la legislazione sulla protezione dei dati[81]. Una violazione del principio della liceità è data, ad esempio, quando dati personali sono elaborati usando violenza, minaccia, negligenza o dolo.

7.7. Principio dell'esattezza dei dati

Secondo il principio dell'esattezza dei dati (art. 7 cpv. 5 LPDP), questi ultimi non possono contenere informazioni false o sbagliate. I dati devono perciò essere corretti, veritieri, completi e aggiornati. Ciò non è il caso se i dati – ad esempio, il luogo, l'orario e/o la data di una videoregistrazione effettuata nell'ambito della sorveglianza pubblica – sono stati manipolati.

---

79 DTF 133 I 77, consid. 5.3 e 5.4.

80 SORO, 2016, pag. 4.

81 ASTRID EPINEY, in Belser/Epiney/Waldmann, Datenschutzrecht, Berna 2011, pag. 518, n. 11 seg.; PHILIPPE MEIER; Protection des données, Berna 2011, pag. 260 n. 637 seg.

7.8. Principio della sicurezza dei dati

La sicurezza dei dati (vedi art. 17 LPDP) implica la protezione dei dati per il tramite di misure tecniche e organizzative intese a proteggere gli stessi dalla perdita, dall'abuso e dal danneggiamento, rispettivamente a garantirne l'integrità, la disponibilità, la confidenzialità e l'autenticità. Più il rischio per l'integrità, la disponibilità e la confidenzialità dei dati è elevato, più elevato deve essere il grado di sicurezza che le misure adottate offrono (approccio basato sui rischi). Gli accorgimenti tecnici devono perciò essere adeguati 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 per i diritti delle persone. La sicurezza dei dati (così come la protezione dei dati in generale) devono essere garantite sin dalla progettazione di un sistema d'elaborazione di dati (*privacy by design*, art. 18 cpv. 1 LPDP). L'implementazione di tecniche che favoriscono la protezione e la sicurezza dei dati (*Privacy Enhancing Technologies*) è un'importante misura di garanzia dei diritti e delle libertà, in particolare del diritto all'autodeterminazione informativa. Tra queste figurano, in particolare, *a)* l'autenticazione personalizzata a due fattori disponibile unicamente al personale autorizzato, con configurazione qualificata del tempo di validità, lunghezza, composizione e non ripetibilità, *b)* la crittografia end-to-end, *c)* il *Backup* di sicurezza, *d)* gli impedimenti fisici di intrusione nei *Data Center*, *e)* gli impianti ridondanti per prevenire l'interruzione di servizio, *f)* la giornalizzazione degli accessi per la ricostruzione di eventi o responsabilità legate all'abuso dei dati, *g)* le certificazioni (in particolare, ISO 27001), *h)* il *Networking* isolato da altre reti (specialmente, da internet pubblico), *i)* le configurazioni adeguate dei *Firewalls* e *l)* il regolare aggiornamento delle misure di sicurezza.

8. Quadro legale della videosorveglianza e delle altre forme di controllo pubblico in Ticino

Attualmente, le principali normative sulla sorveglianza pubblica in Ticino – limitatamente alle forme e strumenti oggetto di questo contributo – sono le seguenti:

- Legge cantonale sulla polizia (art. 9b, 9c e 25 concernenti le registrazioni audio e video per l'identificazione di veicoli, le registrazioni audio e video a supporto operativo e il rispettivo campo di applicazione)[82];
- Regolamento sulle registrazioni audio e video per l'identificazione dei veicoli[83];
- Regolamento per l'impiego di apparecchi audio e video a supporto delle operazioni e degli interventi della polizia cantonale[84];
- Regolamenti comunali sulla videosorveglianza del demanio pubblico.

Quanto ai Regolamenti comunali sulla videosorveglianza del demanio pubblico, va precisato quanto segue:

In virtù dell'autonomia residua comunale (art. 16 cpv. 2 Cost./TI), in ottemperanza ai doveri di polizia locale secondo l'art. 107 della Legge organica comunale[85] e all'obbligo della base legale per elaborazioni sistematiche di dati personali (art. 6 LPDP), attualmente i Comuni ticinesi disciplinano la videosorveglianza del demanio pubblico in regolamenti comunali, che l'Incaricato preavvisa nell'ambito della procedura di approvazione dei regolamenti comunali da parte della Sezione degli enti locali (combinati art. 186 cpv. 2 LOC e 30a lett. f LPDP). L'Incaricato può proporre la modifica dell'atto legislativo, qualora sia ritenuto necessario, in particolare per la sicurezza del diritto o a garanzia dei diritti di personalità e di libertà.

Nel disciplinare la videosorveglianza del demanio pubblico, i Comuni si ispirano perlopiù al regolamento standard[86] e alle rispettive spiegazioni[87] messe a disposizione dall'ICPD. Secondo questi standard, la videosorve-

---

82 Legge sulla polizia del 12 dicembre 1989 (LPol; RL 561.100).

83 Regolamento sulle registrazioni audio e video per l'identificazione dei veicoli del 12 luglio 2011 (RL 561.350).

84 Regolamento per l'impiego di apparecchi audio e video a supporto delle operazioni e degli interventi della polizia cantonale dell'8 febbraio 2012 (RL 561.360).

85 Legge organica comunale del 10 marzo 1987 (LOC; RL 181.100).

86 *https://www4.ti.ch/fileadmin/CAN/SGCDS/ICPD/PDF/TEMI/PDF_Spiegazioni_nuovo_regolamento_standard. pdf.*

87 *https://www4.ti.ch/fileadmin/CAN/SGCDS/ICPD/PDF/TEMI/PDF_Spiegazioni_nuovo_regolamento_standard. pdf.*

glianza del demanio pubblico va distinta da quella del patrimonio amministrativo (immobili amministrativi, strutture pubbliche, scuole, case anziani, ecc.), la quale va disciplinata separatamente in specifici regolamenti di videosorveglianza[88]. Il Regolamento standard limita, poi, la videosorveglianza comunale alle modalità dissuasiva-repressiva e osservativa del traffico e prevede che possa avvenire a tempo indeterminato o determinato, a seconda della portata temporale delle problematiche di sicurezza e ordine pubblico.

Per quanto riguarda la videosorveglianza di singoli beni del patrimonio amministrativo comunale, l'Incaricato ha, per ora, pubblicato unicamente delle direttive sulla videosorveglianza del piazzale scolastico[89]. In esse si sottolinea come la videosorveglianza del piazzale scolastico debba essere valutata e disciplinata in modo differenziato e specifico rispetto alla videosorveglianza del demanio pubblico in generale, tenuto conto del mandato legale affidato alla scuola di sviluppare l'aspirazione di libertà nell'allievo, e dei conseguenti doveri qualificati di parsimonia della videosorveglianza e d'informazione qualificata nei confronti degli allievi. Più in generale, le direttive evidenziano come il piazzale scolastico sia luogo di libertà e svago degli alunni e come, di conseguenza, esso debba di principio essere esente da qualsiasi forma di monitoraggio elettronico, quantomeno nei periodi e orari scolastici. Secondo le direttive, la videosorveglianza potrebbe, eccezionalmente, essere predisposta nei periodi e orari extra-scolastici, qualora altre misure meno incisive nei diritti non dovessero entrare in considerazione. Lo scopo dovrebbe in ogni caso essere limitato alla prevenzione e repressione dei soli reati di natura penale, o comunque di natura qualificata rispetto a infrazioni bagatella (ad esempio, *littering* leggero) e dovrebbero essere rispettati i principi della protezione dei dati, in particolare il principio della trasparenza, secondo il quale gli allievi andrebbero informati in modo trasparente e completo sugli scopi, i luoghi, le tempistiche e le modalità della sorveglianza.

---

88 Altri autori ritengono, invece, che la distinzione tra videosorveglianza del demanio pubblico e del patrimonio amministrativo non sia pertinente e che, di conseguenza, i beni del demanio pubblico e del patrimonio amministrativo vadano assimilati (vedi FLÜCKIGER/AUER, 2006, pag. 926).

89 *https://www4.ti.ch/can/sgcds/pd/temi/videosorveglianza/*.

Quinta parte:
Prassi di sorveglianza pubblica in Ticino, eventuali necessità di adeguamenti legislativi e proposta di legge cantonale quadro sulla videosorveglianza e sulle altre forme di controllo pubblico

9. Prassi e eventuali necessità di adeguamenti legislativi

Con l'avvento di sempre nuove e più sofisticate tecnologie di sorveglianza, con l'espansione territoriale delle reti di videosorveglianza e l'aumento dei beni pubblici sorvegliati, con la diversificazione delle modalità di attuazione della stessa (dissuasiva, osservativa, repressiva o in combinazione) e degli organi responsabili (statali e parastatali cantonali e comunali, di polizia o altro) e con la nuova (e in costante evoluzione) ripartizione dei compiti di polizia prevista dalla legislazione sulla collaborazione fra la Polizia cantonale e le Polizie comunali, l'attuale quadro legale, in particolare per quanto riguarda la ripartizione delle competenze di sorveglianza, non appare più, a mente dello scrivente, come sufficientemente chiaro e completo. Si tratta perciò di garantire, sul piano legislativo, la necessaria chiarezza e sicurezza giuridica circa le varie tecnologie di sorveglianza oggigiorno impiegate, la ripartizione delle competenze di sorveglianza, le modalità e gli scopi del loro impiego (chi fa cosa, con quali strumenti, come e a quale scopo)[90].

In particolare, dalle prassi di consulenza e di vigilanza dell'Incaricato emerge come i Comuni impieghino la videosorveglianza e le altre forme di controllo pubblico in modo eterogeneo. Vi sono Comuni che si limitano alla videosorveglianza dissuasiva degli eco-centri e osservativa del traffico. Altri, invece, hanno introdotto una rete di videosorveglianza capillare, estendendole a scuole, lidi e a altri beni pubblici e si sono dotati

[90] Per quanto riguarda un eventuale deficit normativo nei singoli settori statali e parastatali interessati, non è opportuno che la valutazione dello scrivente venga esposta nel presente contributo. La questione rimane di esclusivo dominio del Gruppo di lavoro sulla sorveglianza pubblica in Ticino, il quale la valuterà al suo interno e ne esporrà, se del caso, le rispettive conclusioni al Consiglio di Stato, sotto forma di rapporto e, eventualmente, di proposta legislativa.

– o intendono farlo – di apparecchi di videosorveglianza mobile (Bodycam e Dashcam). In altri ancora, sono in fase di valutazione e, in taluni casi, già in uso, apparecchi di identificazione automatica delle targhe, per il sanzionamento di contravvenzioni a norme sulla limitazione del traffico locale su strade e parcheggi comunali. Da fonti mediatiche risulta che diversi Comuni si sono già dotati delle necessarie tecnologie di riconoscimento facciale e di profilazione dei movimenti e attendono che dal Cantone arrivi l'autorizzazione per impiegarle. In certi Comuni vi sono stati, in passato, indizi concreti di uso puntuale della videosorveglianza in modalità invasiva e di interfacciamento della videosorveglianza pubblica con quella privata (centri commerciali). Anche singole case anziani comunali attuano la videosorveglianza delle loro strutture[91]. Per quanto riguarda i Consorzi (ad esempio, consorzi di manutenzione di strade montane), alcuni hanno segnalato all'Incaricato di effettuare della videosorveglianza dissuasiva per il controllo del rispetto di limitazioni del traffico su strade riservate agli aventi diritto. Dal canto loro, alcune Chiese ufficialmente riconosciute hanno segnalato all'Incaricato, nell'ambito delle sue attività di consulenza, di effettuare della videosorveglianza in modalità dissuasiva a tutela della sicurezza dell'edificio ecclesiastico o di strutture attigue. A livello cantonale, dalla prassi dell'Incaricato risulta che vari organi e settori dello Stato e del parastato attuano la videosorveglianza dissuasiva o osservativa di stabili e altri beni amministrativi (parcheggi, ecc.). Per quanto riguarda la Polizia cantonale, è notorio e desumibile dal diritto positivo che essa svolge svariati tipi di sorveglianza e di controllo pubblici e, laddove necessario, lo fa in collaborazione con diversi altri organi partecipanti federali e di altri Cantoni.

10. Nuova legge cantonale quadro sulla sorveglianza pubblica?

L'eterogeneità delle prassi di sorveglianza pubblica esposte nel capitolo precedente ripropone la questione della necessità di una legislazione

[91] Da questa panoramica risulta come l'autonomia comunale – che concede ai Comuni la facoltà di legiferare entro i limiti posti dalla Costituzione e dalle leggi – venga interpretata in modo assai discrezionale, sebbene il diritto positivo non attribuisca ancora chiare competenze di sorveglianza pubblica ai Comuni.

cantonale quadro sulla videosorveglianza e sulle altre forme di controllo pubblico in Ticino. Tale questione era stata valutata una prima volta già nel 2009 dall'allora Incaricato cantonale della protezione dei dati il quale, in risposta ad un'interrogazione parlamentare[92], proponeva di rinunciare all'adozione di una disposizione cantonale quadro sulla videosorveglianza nella legge sulla protezione dei dati personali e di lasciarne ai Comuni, in virtù della competenza residua, la competenza legislativa nel loro diritto speciale[93]. L'interrogazione chiedeva di prevedere delle norme cantonali quadro minime in materia di videosorveglianza degli spazi pubblici, nel rispetto dell'autonomia legislativa comunale, indipendentemente dalla *sedes materiae* (ad esempio, la LPDP, la LOC o una nuova legge cantonale quadro sulla videosorveglianza, sul modello della legge sulla protezione dei dati nel settore della polizia[94]). L'essenziale, secondo gli iniziativisti, era che il Gran Consiglio fosse chiamato a legiferare, definendo in particolare l'organo comunale responsabile, l'oggetto, le modalità e i tempi della videosorveglianza, l'autorizzazione o meno per la videoregistrazione, la durata di conservazione dei dati, la comunicazione delle registrazioni a terzi, i diritti delle persone interessate e il ruolo dell'Incaricato.

Nella sua valutazione, l'allora Incaricato aveva concluso:

> «(…) l'adozione di una disposizione cantonale quadro sulla videosorveglianza nella legge sulla protezione dei dati personali non è necessaria. L'ente pubblico che intende impiegare un sistema di videosorveglianza dissuasiva deve, in ogni caso, dotarsi delle necessarie basi legali, come per qualsiasi attività o compito che è chiamato a svolgere. È nel diritto speciale che la materia va disciplinata. Per quanto riguarda i Comuni la situazione

---

92 Interrogazione parlamentare Manuele Bertoli e cofirmatari n. 317.09 del 25 novembre 2009 denominata «Base legale cantonale per la videosorveglianza degli spazi pubblici: sì o no?»

93 MICHELE ALBERTINI, Videosorveglianza degli spazi pubblici: una base legale quadro cantonale è necessaria? Rapporto del 17 dicembre 2009 sull'interrogazione n. 317.09 del 25 novembre 2009 presentata dal deputato Manuele Bertoli e cofirmatari denominata «Base legale cantonale per la videosorveglianza degli spazi pubblici: sì o no? *https://www4.ti.ch/fileadmin/CAN/SGCDS/ICPD/PDF/TEMI/Videosorveglianza_rapporto_ICPD_12 2009. pdf.*

94 Legge sulla protezione dei dati personali elaborati dalla polizia cantonale e dalle polizie comunali del 13 dicembre 1999 (LDPpol; RL 163.150).

> può essere mantenuta, perché conforme all'ordinamento costituzionale vigente: in virtù della competenza residua essi rimangono competenti in materia e, se intenzionati ad impiegare la videosorveglianza sul proprio territorio giurisdizionale, devono dotarsi di una specifica base giuridica formale, ossia di una disposizione in un regolamento comunale esistente o di un regolamento comunale ad hoc (…). In assenza di una base legale cantonale (generale), e in virtù del regime di competenze disciplinato dai combinati art. 16 della Costituzione della Repubblica e Cantone Ticino del 14 dicembre 1997 (Cost./TI; RL 1.1.1.1) e 2 della legge organica comunale del 10 marzo 1987 (LOC; RL 2.1.1.2) che stabiliscono la competenza residua dei Comuni, questi ultimi sono competenti a regolamentare la videosorveglianza dissuasiva sul proprio territorio giurisdizionale (ad eccezione degli spazi privati). Ciò significa che l'ente pubblico comunale che intendesse dotarsi di un sistema di videosorveglianza del proprio territorio giurisdizionale deve preventivamente emanare una normativa specifica. Considerati gli argomenti illustrati nel rapporto, in particolare i rischi di ingerenza nei diritti fondamentali derivanti dall'uso di tecnologie sempre più sofisticate, come pure le tendenze normative ad ogni livello, la soluzione più indicata è quella del regolamento comunale (quindi una legge in senso formale)».

Nel 2016 è poi stato introdotto nella LPDP l'obbligo generale di legiferare in materia di elaborazioni sistematiche di dati (e quindi anche di sorveglianza pubblica) e sono state definite le esigenze che le basi legali devono adempiere. Secondo tale modifica legislativa va previsto, tra l'altro, l'oggetto e lo scopo dell'elaborazione, l'organo responsabile, gli organi partecipanti e gli utenti, i destinatari di dati, le modalità e le condizioni, la cerchia delle persone interessate, la durata della conservazione dei dati e le misure di sicurezza (art. 6 LPDP). La norma prevede inoltre che le basi legali debbano essere di rango formale, qualora i dati elaborati siano meritevoli di particolare protezione[95].

Seguendo la risposta del Cantone all'interrogazione parlamentare in questione e in ottemperanza all'art. 6 LPDP, oggigiorno i Comuni che intendono dotarsi di videosorveglianza per il monitoraggio del loro demanio pubblico emanano specifici regolamenti.

---

[95] Vedi Messaggio n. 7061 del 18 marzo 2015 sulla modifica della Legge sulla protezione dei dati personali del 9 marzo 1987 (LPDP) riguardante i motivi giustificativi e i principi che reggono l'elaborazione di dati personali (art. 6 e 7 LPDP), *https://www4.ti.ch/fileadmin/CAN/SGCDS/ICPD/PDF/DIRITTO_TI/m7061_01.pdf.*

Nel frattempo però, come già visto, la sorveglianza pubblica non si limita più al monitoraggio grandangolare e dissuasivo del demanio pubblico tramite videocamere fisse di sorveglianza. Nuove, performanti tecnologie come le Bodycam, gli apparecchi di lettura targhe e le applicazioni di riconoscimento facciale e di movimento si sono aggiunte e le stesse videocamere di sorveglianza hanno subito rapide e importanti evoluzioni tecnologiche che le hanno rese potenzialmente iperintrusive. Il tutto su perimetri territoriali sempre più estesi, con organi responsabili sempre più numerosi e differenziati e con modalità di sorveglianza sempre più diversificate. Se si aggiungono a ciò la nuova e più ampia attribuzione di compiti alle polizie locali prevista dalla legislazione cantonale sulla collaborazione fra la polizia cantonale e le polizia comunali[96], l'eterogeneità dell'impiego delle tecnologie di sorveglianza e le velleità di alcuni Comuni di sfruttare ogni possibilità offerta dalle tecnologie per spingere verso una sorveglianza sempre più completa, la conclusione è chiara: il panorama, le dinamiche e le problematiche che ne emergono sono radicalmente cambiate rispetto al 2009 e la riapertura della questione su una nuova legge cantonale quadro sulla sorveglianza pubblica è quantomeno opportuna. La stessa interrogazione parlamentare del 2009 chiedeva che si legiferasse sulla materia a livello cantonale.

Alla stessa stregua di quanto avvenuto in altri Cantoni[97], la promulgazione di una legge cantonale quadro ticinese sulla sorveglianza pubblica permetterebbe innanzitutto di uniformare le prassi eterogenee attualmente presenti sul territorio e di colmare, per il resto, le attuali lacune legislative prevedendo, in una prima parte, in modo chiaro, uniforme e trasversale, le definizioni e i principi comuni applicabili all'insieme di tecnologie di sorveglianza e di organi statali e parastatali cantonali e locali che oggigiorno attuano in una qualche forma la sorveglianza pubblica e disciplinando, in una seconda parte, aspetti peculiari ai singoli settori di competenza (Polizia cantonale, Comuni e Patriziati, enti parastatali e

[96] Legge sulla collaborazione fra la polizia cantonale e le polizie comunali del 16 marzo 2011 (LCPol; RL 563.100).

[97] Ad esempio, Canton Friborgo, Loi sur la vidéosurveillance du 7 décembre 2010 (LVid; RSF 17.3).

Chiese). Elevando gli attuali regolamenti comunali sulla videosorveglianza pubblica in una legge cantonale quadro, si centralizzerebbero presso il Legislatore cantonale le competenze decisionali in materia, sia dei Comuni, sia dell'Incaricato, il quale, con il suo regolamento standard e le sue direttive, orienta e decide oggigiorno ampiamente, di fatto, la materia. Nel complesso, una simile dinamica legislativa – che dovrebbe comunque garantire ancora una certa autonomia comunale – favorirebbe sia una maggiore sicurezza del diritto, sia una migliore e da più parti auspicata economia del diritto tra Cantone e Comuni.

11. Riflessioni e primi spunti normativi per una nuova legge cantonale quadro sulla sorveglianza pubblica

Qui di seguito vengono esposti alcuni primi spunti normativi per una eventuale, futura legge cantonale quadro sulla videosorveglianza e su altre forme di controllo pubblico. Si tratta di una possibile indicazione su aspetti generali della sorveglianza pubblica che possono, di principio, essere considerati pacifici, poiché deducibili dai principi generali del diritto e dall'attuale legislazione sulla protezione dei dati, ma che non sono ancora adeguatamente concretati dal diritto positivo per il settore della sorveglianza pubblica. Per quanto riguarda le eventuali norme speciali per le singole tecnologie, settori e autorità coinvolte nella sorveglianza pubblica, esse andranno, se del caso, proposte dalle autorità coinvolte nel rispettivo iter legislativo e rappresentate nel Gruppo di lavoro sulla sorveglianza pubblica in Ticino (tenendo conto in particolare delle condizioni poste dall'art. 6 cpv. 3 LPDP concernente il contenuto minimo delle basi legali per le elaborazioni sistematiche di dati personali), nel caso in cui si giungesse alla conclusione di voler sottoporre al Consiglio di Stato un progetto in tal senso.

11.1. Spunti normativi

I seguenti spunti normativi si limitano, perciò, a prevedere:

a) Le norme generali e trasversali concernenti lo scopo della legge, il campo di applicazione, il rapporto con altre leggi, le principali defini-

zioni, le condizioni per l'introduzione di nuove tecnologie di sorveglianza, i principi generali e i diritti delle persone interessate;

b) La riserva della legislazione sulla polizia quale sede legislativa per le norme speciali sulla sorveglianza pubblica attuata dalla stessa;

c) Alcune delle principali norme sulla videosorveglianza pubblica da parte dei Comuni, nella misura in cui risultano già sind'ora, di principio, pacifiche.

11.2. Primi spunti normativi per una legge cantonale quadro sulla videosorveglianza e su altre forme di controllo pubblico

Capitolo primo
Norme generali e definizioni

Scopo

[1]La presente legge ha lo scopo di proteggere i diritti e le libertà fondamentali, in particolare i diritti di libertà e di protezione dei dati personali, delle persone soggette a videosorveglianza o a altre forme di controllo nei luoghi pubblici da parte dei soggetti di cui all'articolo seguente.

[2]Essa fissa le condizioni e le modalità della videosorveglianza e delle altre forme di controllo pubblico.

Campo di applicazione

La presente legge si applica alla videosorveglianza e a altre forme di controllo pubblico da parte di organi statali e parastatali cantonali e locali e delle Chiese ufficialmente riconosciute dallo Stato che attuano la sorveglianza.

Riserva di altre leggi

Per aspetti della sorveglianza 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 del 9 marzo 1987 (RLPDP).

Definizioni

Ai sensi della presente legge, i seguenti termini significano:

a. Videosorveglianza osservativa: attività di vigilare, a lungo termine, su un luogo o un bene amministrativo pubblico a distanza, tramite una rete di videocamere a postazione fissa, con un campo di visione grandangolare circoscritto a uno specifico bene pubblico d'uso comune, con apparecchi in grado di raccogliere segnali d'immagini e di trasmetterli a una centrale di sorveglianza per visione in tempo reale, in chiaro e, di norma, senza registrazione d'immagini. È finalizzata alla supervisione e, se del caso, al ripristino, del corretto flusso del traffico di autoveicoli in seguito a disturbi, disfunzioni o pericoli e, in determinate circostanze, alla supervisione in tempo reale di flussi o assembramenti di persone, a supporto e ottimizzazione dell'attività di polizia in loco, oppure per il controllo in tempo reale degli accessi a beni pubblici d'uso comune;
b. Videosorveglianza dissuasiva: attività di vigilare, a lungo termine, su un luogo o un bene amministrativo pubblico a distanza, tramite una rete di videocamere a postazione fissa, possibilmente con schermatura di beni tutelati (privacy filters), con apparecchi a campo di visione grandangolare circoscritto a uno specifico bene pubblico d'uso comune, in grado di raccogliere segnali d'immagine e di trasmetterli a una centrale di sorveglianza, per loro registra-

zione e conservazione per una durata prestabilita. Lo scopo consiste nella prevenzione di minacce e turbamenti alla sicurezza e all'ordine pubblico in circostanze di criminalità diffusa, tramite la posa ben riconoscibile di videocamere di sorveglianza e per la ricostruzione e il perseguimento di infrazioni di carattere penale tramite analisi delle immagini successiva alla loro commissione.

La videosorveglianza dissuasiva può avvenire anche a breve termine, in situazioni e luoghi che presentano una criticità momentanea per la sicurezza e l'ordine pubblico. Può essere attuata segnatamente tramite videocamere mobili all'uniforme dell'agente di polizia (bodycam), attivate in situazioni pericolose per la sicurezza dell'agente stesso o delle persone coinvolte in operazioni di polizia. Ha scopo dissuasivo su persone coinvolte e agenti di polizia grazie alla registrazioni di immagini e suoni che, in caso di necessità, possono essere analizzate e utilizzate successivamente come mezzi di prova;

c. Videosorveglianza invasiva: attività di vigilare, a breve termine, su un luogo o un bene amministrativo pubblico a distanza, tramite videocamera o rete di videocamere a postazione fissa o mobile, con un campo di visione circoscritto su una o più persone specifiche, in tempo reale, in chiaro, con o senza registrazione d'immagini, indipendentemente dalla presenza di un pericolo o di una minaccia concreta, in circostanze specifiche e qualificate dal punto di vista della sicurezza, ad esempio in occasione di manifestazioni pubbliche e manifestazioni a rischio violenza oppure in situazioni pericolose per la sicurezza dell'agente stesso o delle persone coinvolte in operazioni della polizia. È finalizzata al tempestivo riconoscimento di eventi illeciti o delittuosi di carattere penale in atto o alla loro prevenzione e all'intervento immediato delle forze dell'ordine;

d. Riconoscimento facciale: tecnica d'identificazione di una persona a partire da una o più immagini che ne ritraggono il volto, basata sull'analisi di caratteristiche visibili dello stesso, date dal loro ordine geometrico e dalle caratteristiche della superficie della pelle. Presuppone una raccolta originaria di immagini salvate in un formato particolare (template) in una specifica banca dati e successivamente paragonate con le immagini riprese da una videocamera. Il riconoscimento facciale è predisposto per l'inseguimento e tracciamento, anche in tempo reale, di persone, nell'ambito del perseguimento di eventi illeciti o delittuosi di carattere penale o della loro prevenzione. Può tecnicamente essere integrata momentaneamente a una videocamera o a una rete di videocamere predisposte per la videosorveglianza a lungo termine;

e. Strumenti di lettura e identificazione di targhe di veicoli: strumenti fissi o mobili per lettura e identificazione, tramite telecamera, di lettere e numeri di targhe di veicoli, nonché per registrazione di orario, posizione e direzione del veicolo, e per confronto automatico con banche dati di targhe. Sono finalizzati alla ricerca di veicoli scomparsi, rubati o coinvolti in reati o che trasportano merci pericolose, al controllo del transito di veicoli su strade a traffico limitato o al controllo dell'accesso a posteggi con barriera o a altri siti ad accesso limitato.

Condizioni per l'introduzione di tecnologie di sorveglianza

[1]L'introduzione di nuove tecnologie o applicazioni di sorveglianza pubblica deve essere giustificata da un interesse pubblico preponderante e deve essere preceduta da:

a) Valutazione dell'idoneità, efficacia e necessità, segnatamente tramite test pilota, per l'esecuzione degli specifici compiti legali in questione;

b) Analisi d'impatto sui diritti e sulle libertà del cittadino;
c) In caso di adempimento delle condizioni di cui ad a) e b), regolamentazione nel diritto formale e materiale d'esecuzione.

[2]Riservati i principi generali di cui al presente capitolo, l'interesse pubblico della sicurezza e dell'ordine pubblico può, di principio, essere riconosciuto, quando è data una situazione di pericolo di commissione di atti illeciti a carattere penale oggettivamente motivabile, quale un pericolo concreto per la sicurezza o un punto cruciale di criminalità.

[3]L'interesse pubblico non è dato quando sussiste unicamente un generico motivo di sicurezza e ordine pubblico, rispettivamente quando sussiste unicamente un rischio generale e astratto.

Interesse pubblico, principi e diritti della protezione dei dati

Principio della liceità

Una limitazione dei diritti costituzionali tramite videosorveglianza o altre forme di controllo pubblico è accettabile unicamente nella misura in cui sia rispettato l'insieme del diritto, in particolare i diritti costituzionali e i principi generali, e sia dato un interesse pubblico preponderante.

Principio della sostenibilità

La videosorveglianza e le altre forme di controllo pubblico previste dalla presente legge devono essere impiegate nella maniera più utile in termini di prevenzione e più sostenibile sotto il profilo democratico e dei diritti fondamentali.

Principio della proporzionalità

[1]La videosorveglianza e le altre forme di controllo pubblico devono essere idonee e necessarie alla sicurezza e l'ordine pubblico e deve sussistere un rapporto ragionevole di grandezza tra tale scopo e la restrizione dei diritti di libertà, di autodeterminazione e di protezione dei dati che ne risulta (criterio della pertinenza e non eccedenza).

[2]In particolare, la videosorveglianza e le altre forme di controllo pubblico devono essere pertinenti e non eccedenti rispetto a:
a. Compito legale dell'organo responsabile;
b. Tipologia di illeciti perseguiti;
c. Modalità di sorveglianza;
d. Categorie di dati personali elaborati;
e. Cerchia di persone interessate;
f. Estensione temporale;
g. Estensione territoriale;
h. Angolo visuale;
i. Grado di dettaglio e ingrandimento delle immagini;
l. Durata di conservazione dei dati;
m. Cerchia di personale abilitato alla gestione e all'accesso agli impianti di videosorveglianza, ai programmi informatici ivi correlati e alle immagini registrate.

[3]La videosorveglianza e le altre forme di controllo pubblico sono sproporzionate 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;
b. Implicano l'elaborazione sistematica di dati personali e di dati identificativi, sebbene le finalità perseguite possano essere raggiunte mediante dati anonimi o opportune modalità che permettano di identificare l'interessato solo in caso di necessità (privacy filters);

c. Le infrazioni perseguite non si limitano a infrazioni di natura penale o infrazioni amministrative qualificate, ma concernono anche contravvenzioni amministrative minori;
d. Concernono determinati gruppi di persone, al fine di sorvegliarli o emarginarli, senza che sia dato un punto cruciale di criminalità;
e. Avvengono alla ricerca di possibili reati, in assenza di un sospetto concreto, oppure implicano la raccolta preventiva di dati, senza che vi sia un chiaro e concreto scopo di elaborazione (Fishing Expedition).

[4] La videosorveglianza va periodicamente rivalutata nella proporzionalità.

Principio della trasparenza

Le persone interessate devono essere adeguatamente informate sull'impiego di strumenti di sorveglianza e di controllo pubblico, segnatamente sullo scopo, sulle modalità d'impiego, sui dati elaborati, sull'organo responsabile e sui diritti di protezione dei dati.

Principio della finalità

A tutela della fiducia del cittadino nello scopo dell'elaborazione legalmente previsto o deducibile dalle circostanze concrete, i dati personali elaborati tramite videosorveglianza o altre forme di controllo pubblico non possono essere utilizzati o trasmessi per uno scopo che, secondo la buona fede, sarebbe incompatibile con quello per il quale originariamente erano stati raccolti.

Principio dell'esattezza dei dati

I dati elaborati tramite videosorveglianza o altre forme di controllo pubblico devono essere esatti, vale a dire corretti, veritieri, completi e aggiornati.

Principio della sicurezza dei dati

[1]Gli organi responsabili devono garantire, sin dalla progettazione di un sistema di sorveglianza 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.

[2]Le 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.

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

Diritti della protezione dei dati

I diritti della protezione dei dati personali sono garantiti conformemente alla legge sulla protezione dei dati personali del 9 marzo 1987.

Capitolo secondo
Norme settoriali

Organi statali e parastatali cantonali
Polizia cantonale

Diritto applicabile

Alla sorveglianza da parte della Polizia cantonale si applica la legislazione sulla polizia e, sussidiariamente, le norme generali e le definizioni previste dal capitolo primo della presente legge.

Organi statali e parastatali locali
Comuni e Consorzi di Comuni

Scopo della videosorveglianza

La videosorveglianza avviene a supporto dell'esecuzione delle funzioni di polizia comunale attinenti alla prevenzione e al perseguimento di illeciti di natura penale o amministrativa qualificata, nonché per la gestione del traffico.

Modalità di videosorveglianza	La videosorveglianza avviene nelle modalità dissuasiva oppure osservativa del traffico.
Videosorveglianza del sedime scolastico	Se la videosorveglianza risulta essere necessaria per la prevenzione e la repressione di reati di natura penale o amministrativa qualificata, essa può essere predisposta per la sorveglianza del sedime scolastico in modalità dissuasiva e in periodi e orari extra-scolastici.
Trasparenza	[1]Il Comune garantisce un'adeguata informazione sulla presenza di videocamere, sulla modalità di sorveglianza e sull'organo responsabile, segnatamente con cartelli indicatori possibilmente in prossimità delle singole videocamere. [2]In caso di videosorveglianza del sedime scolastico, gli allievi devono essere informati in modo trasparente e completo anche sugli scopi, i luoghi, le tempistiche e le modalità.
Trasmissione di dati a terzi	[1]Di principio, le videoregistrazioni non sono trasmesse a terzi. [2]Nel caso di procedimenti civili, penali o amministrativi, le videoregistrazioni 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.
Durata di conservazione, anonimizzazione e distruzione delle immagini	[1]I Comuni definiscono la durata di conservazione in funzione delle effettive necessità per la ricostruzione di eventi e responsabilità. [2]È riservata la conservazione di una copia delle videoregistrazioni in caso di procedura civile, penale o amministrativa, fino a conclusione della stessa.
Organo responsabile	[1]Il Municipio è l'organo responsabile della videosorveglianza ai sensi dell'art. 4 cpv. 6 LPDP. [2]Esso può emanare le disposizioni necessarie all'esecuzione della presente legge. Definisce, in particolare, il servizio comunale o il mandatario incaricato di eseguire la videosorveglianza, i luoghi soggetti a videosorveglianza, le ulteriori modalità e le condizioni della videosorveglianza, i diritti di accesso alle registrazioni e le misure di sicurezza a tutela della loro autenticità, confidenzialità e integrità. [3] Vigila sulla corretta applicazione e sul rispetto della presente legge.

Conclusioni

Nell'ambito dei diritti di libertà e di protezione dei dati, la Costituzione e la legislazione sulla protezione dei dati sono peculiarmente destinate a stabilire le regole, non le nuove tecnologie e i loro venditori. Non tutto quello che è tecnicamente possibile lo è anche giuridicamente. Lo Stato è chiamato a tenersi entro i parametri legali e costituzionali, in particolare i principi della legalità, della proporzionalità e della causalità, senza lasciarsi eccessivamente sedurre e accecare dalle possibilità tecniche offerte dalle nuove tecnologie di videosorveglianza e di interfacciamento delle banche dati, e nemmeno senza fondarsi eccessivamente sulla paura per il crimine, diventata oramai in certi Paesi elemento strutturale della

società, nonché senza spostare eccessivamente i limiti della prevenzione lontano dal pericolo o sospetto concreto. Ciò, al fine di evitare che – in un paradossale stravolgimento delle logiche di diritto – siano le libertà fondamentali a doversi improvvisamente giustificare nei confronti delle nuove tecnologie di sicurezza, e non viceversa[98]. Altrimenti detto, bisogna evitare di arrivare allo scambio radicale tra sicurezza e libertà. Non c'è la possibilità, in democrazia, di scambiare alcunché su questo terreno[99]. Nessuno vuole vivere negli estremi, ossia nella privacy totale – che genererebbe insicurezza –, oppure nello stato della massima trasparenza del cittadino, che metterebbe a rischio democrazia e libertà[100]. Il rischio di questo stravolgimento dei valori in gioco è però già radicato nell'obiezione giustificativa che si sente spesso evocare secondo cui, se non si ha nulla da nascondere, non v'è ragione di preoccuparsi per la sorveglianza e la raccolta di dati. Questa affermazione è fondamentalmente sbagliata, poiché anche non avendo nulla da nascondere, il cittadino ha il diritto – costituzionale – di vivere liberamente, senza doversi sentire in un qualche modo costantemente sorvegliato e documentato. Insomma, va contenuta la capacità invasiva della sorveglianza pubblica nella sfera di libertà entro i confini invalicabili prescritti dalla Costituzione[101] e va rinnovata l'educazione e l'inclinazione per la libertà. Non possiamo rassegnarci a fare il lutto di parte della nostra libertà, anche se la casistica in ambito di sorveglianza pubblica conferma un cambiamento epocale in questo senso[102]. La democrazia deve ripresentarsi oggi in maniera solida, non come modello istituzionale sempre più resiliente, duttile e adattabile. Perciò, anche di fronte alla legittima esigenza di rafforzare la sicurezza e la prevenzione tramite misure di sorveglianza, occorre sempre privilegiare la tutela dei diritti fondamentali rispetto all'uso di strumenti investigativi

98 Va evitata, in particolare, l'introduzione di tecnologie di sorveglianza, quali il riconoscimento facciale, senza che vi sia la necessaria legittimità democratica e giuridica. Vedi in proposito, SIMMLER/CANOVA, 2021, pag. 116.

99 MARCO MINNITI, Convegno Roma 2016, pag. 94.

100 AUGUSTA IANNINI, Convegno Roma 2016, pag. 15.

101 ARMANDO SPATARO, Convegno Roma 2016, pag. 41.

102 MARTENET/DUBEY, 2021, pag. 518, n. 76.

ultra performanti[103]. Bisogna anche interrogarsi sul reale interesse pubblico e la reale necessità della sorveglianza pubblica, tenuto conto del fatto che, come detto, usata in determinate modalità, può violare gravemente i diritti fondamentali[104]. Ne consegue che – ed è quanto si è voluto sottolineare in questo contributo – la sorveglianza pubblica deve limitarsi alla prevenzione generale e non enfatizzare i pericoli.

Vanno nel contempo rafforzati i poteri giurisdizionali e le autorità di vigilanza sul rispetto dei diritti e delle libertà (tra le quali, le autorità di protezione dei dati); va evitato che si spostino continuamente ed eccessivamente i limiti nelle politiche di sicurezza e va riorientata la percezione di stato d'allerta costante verso sempre maggiore oggettività. Va, poi, costantemente migliorata la prevenzione del crimine tramite la (ri-) educazione della società, in particolare dei suoi membri più deboli, evitando nel contempo che un certo flop educativo diventi anche – a causa di una sorveglianza eccessiva – un'emergenza democratica. In attuazione del principio della legalità, al Legislatore vanno infine sottoposti, precedentemente alla messa in atto di qualsiasi nuovo sistema o applicazione di sorveglianza, le necessarie proposte normative, che vanno a loro volta sempre precedute da un attento esame dell'adempimento delle condizioni poste dalla Costituzione e dalle leggi per la restrizione lecita di diritti e libertà costituzionali e da un'analisi d'impatto della sorveglianza su tali diritti. Se del caso, il progetto di sorveglianza va rimpiazzato con misure meno incisive nei diritti. Le buone prassi in ambito di protezione dei dati (realizzabili, ad esempio, con dei *Good Privacy Label* per i Comuni) potrebbero mitigare l'impatto della sorveglianza sull'opinione pubblica e costituire peraltro anche un nuovo, interessante fattore di promozione del nostro territorio.

[103] GIAN DOMENICO CAIAZZA, Convegno Roma 2016, pag. 154.

[104] RÜEGG, FLÜCKIGER, NOVEMBER, KLAUSER, 2006, pag. 22.