dell'Arma dei Carabinieri
Rassegna

Scuola Ufficiali Carabinieri

4

Anno LXX - ottobre / dicembre 2023

POLIGRAFICO E ZECCA DELLO STATO ITALIANO
IPZS S.p.A.

Caratteristiche
Periodico trimestrale a carattere tecnico-scientifico-professionale a cura della Scuola Ufficiali Carabinieri
Proprietario ed Editore Ministero della Difesa
Iscritto nel Registro della Stampa del Tribunale di Roma al n. 305/2011 in data 27-X-2011
Diffuso attraverso la rete internet sul sito Istituzionale dal Service Provider "Fastweb S.p.A." - Milano
https://www.carabinieri.it/media---comunicazione/rassegna-dell-arma/la-rassegna
ISSN (on-line): 2533-3070 - ISSN (print): 0485-3997

Rassegna dell'Arma dei Carabinieri

4
Anno LXX
ottobre - dicembre 2023

MINISTERO DELLA DIFESA

anvur
Agenzia Nazionale di Valutazione del sistema Universitario e della Ricerca
National Agency for the Evaluation of Universities and Research Institutes

POLIGRAFICO E ZECCA DELLO STATO ITALIANO
IPZS S.p.A.

dell'Arma dei Carabinieri
Rassegna

SOMMARIO n. 4
ottobre - dicembre 2023

SOMMARIO n. 4
ottobre - dicembre 2023

Scientiae

Informazioni e Segnalazioni

25 novembre 2023

Convegni

Libri

Inserto

Flusso di capitali illeciti
Azioni di contrasto

Dottore
Andrea Mario Trentini(*)

Sottotenente
Giuseppe De Martino(**)

Videosorveglianza e tutela della *privacy* e nelle *smart city*

L'articolo affronta l'evoluzione dei centri abitati e le complesse sfide gestionali che gli amministratori devono affrontare in una città moderna. Si evidenzia l'importanza di garantire servizi efficienti, inclusi quelli digitali, dalla salute alla sicurezza. Il progresso tecnologico, con l'impiego delle tecnologie informatiche, ha migliorato la qualità della vita e favorito il concetto di Smart City. Nell'articolo "Percezione della sicurezza nelle Smart City" viene menzionato uno studio dell'IESE Business School che classifica le Smart City in base a vari criteri. In questo articolo viene incluso un ulteriore fattore, la percezione della sicurezza legata alla videosorveglianza. Si sottolinea anche l'importanza di rispettare la normativa sulla privacy nell'utilizzo dei sistemi di videosorveglianza urbana per trovare un equilibrio tra sicurezza e privacy per i cittadini.

The article addresses the evolution of urban centers and the complex management challenges that administrators must face in modern city. It highlights the importance of ensuring efficient services, including digital ones, ranging from health to security. Technological progress, through the use of information technologies, has improved the quality of life and promoted the concept of Smart Cities. In the article «Perception of Security in Smart Cities,» a study by the IESE Business School is mentioned, which classifies Smart Cities based on various criteria. This article includes an additional factor, the perception of security related to video surveillance. It also emphasizes the importance of complying with privacy regulations in the use of urban surveillance systems to strike a balance between security and privacy for citizens.

(*) Ricercatore - Professore Aggregato del Dipartimento di Informatica "Gianni degli Antoni", Milano.
(**) Software Engineer Expert in Par-Tec SPA. Executive Ph. D. Student all'Università di Milano, già Sottotenente della Riserva Selezionata in congedo.

SOMMARIO: 1. Sorveglianza e videosorveglianza nelle *Smart City*. - 2 Suddivisione dei ruoli tra Amministrazione locale e Polizia locale. -3 Città italiane videosorvegliate. - 4 Confronto fra tecniche di videosorveglianza fra Europa, USA e Cina. - 5 Conclusioni.

1. Sorveglianza e videosorveglianza nelle *Smart City*

Per sorveglianza si intende un costante controllo diretto o indiretto su uno o più individui a scopo cautelativo o preventivo. Fin dal medioevo, i cittadini europei sovrintendevano alla sicurezza delle mura urbane, ad esempio, con costanti ronde organizzate. Questo fenomeno ha portato, nel tempo, alla formazione di un vero e proprio corpo di polizia locale. Nel 1829, per rafforzare il mantenimento dell'ordine pubblico, in Gran Bretagna venne istituita tramite il *Metropolitan Police Act* una forza, volutamente non armata, con una divisa non militarizzata visibile a tutti. Uno dei compiti della *Metropolitan Police* era proprio quello di identificare coloro che turbavano la sicurezza pubblica e che non potevano essere sotto stretto controllo da parte delle forze di polizia standard [16].

Sempre in Gran Bretagna, il connubio tra l'esigenza di monitorare soggetti ritenuti pericolosi e l'impiego di mezzi e risorse ha caratterizzato il XVII secolo: come misura cautelativa, le politiche dell'epoca volevano il trasferimento di questi particolari soggetti in zone sicure e ben monitorate. In questo scenario, il filosofo Jeremy Bentham escogita il *Panopticon or the Inspection House* ovvero un ipotetico istituto penitenziario basato sul principio fondamentale dell'utilitarismo. L'obiettivo del *Panopticon* era di poter sorvegliare il massimo numero di detenuti con l'impiego di pochissime persone (o forse una), con la peculiarità di poter nascondere il sorvegliante dal sorvegliato. In figura 1 il progetto del *Panopticon*.

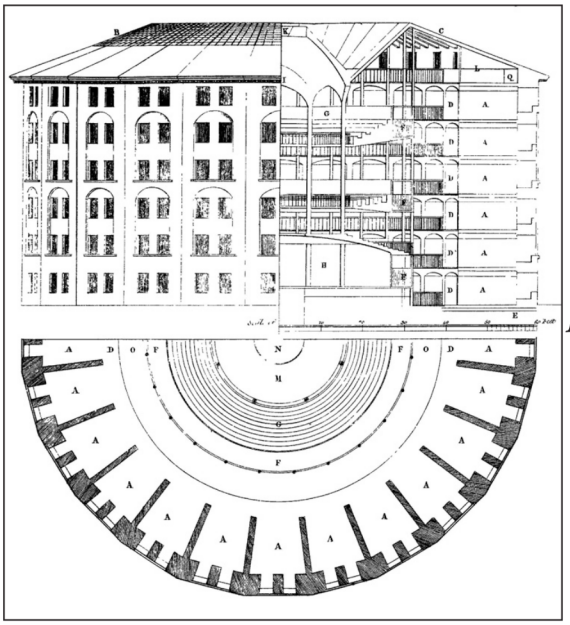

Figura 5: *Progetto di Panopticon, 1791 da wikipedia.org*

Oggi il concetto del Panopticon viene utilizzato in tutto il mondo per descrivere una situazione (tipicamente nel mondo digitale) aberrante di sorveglianza pervasiva, invasiva e inutile.

Infatti, dalla metà del XX secolo, la sorveglianza si è evoluta diventando oggetto principale di veri e propri programmi governativi (segreti) di sorveglianza di massa. Tra i più famosi ricordiamo il programma ECHELON (dal francese *scaglione*) attuato negli anni Quaranta istituito tra gli stati membri dell'UKUSA(1).

Questo programma consiste in una maxi-rete di spionaggio elettronico mondiale, con obiettivo di raccogliere informazioni tramite *SIGINT*, acronimo di SIGnals INTelligence, provenienti da canali elettromagnetici o comunicazioni radio che evolvendosi nel tempo, sono in grado di intercettare telefonate, fax, e-mail in ogni angolo del pianeta [2][8].

Un altro programma di sorveglianza globale molto famoso è il PRISM, iniziato nel 2007 in USA sotto l'amministrazione del presidente G.W. Bush a seguito dell'introduzione del *Protect American Act*, che a sua volta introduce delle modifiche al *FISA Foreign Intelligence Surveillance Act*, la legge per la sorveglianza fisica ed elettronica e per la raccolta delle informazioni delle intelligence straniere [4].

La peculiarità di questi programmi è la loro segretezza: sono stati raccolti dati e metadati su milioni di persone (dai semplici cittadini fino alle più alte cariche istituzionali) in tutto il mondo senza che queste ne fossero informate, e quindi di fatto senza alcun mandato o autorizzazione a farlo, violando la loro *privacy*.

Nel mondo della sorveglianza, lo strumento più diffuso è quello della videosorveglianza, ovvero la sorveglianza (preventiva, in assenza di mandati giudiziari) di aree pubbliche o private effettuata tramite riprese da videocamere, nelle *Smart City* e non solo, con diverse finalità tra cui [12]:

➢ *protezione e controllo della proprietà pubblica o privata;*

➢ *rilevazione, prevenzione e controllo di eventuali infrazioni: attività svolta dai soggetti pubblici nel quadro delle competenze ad essi attribuite dalla legge;*

➢ *acquisizione di prove a seguito di atti illeciti;*

➢ *protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati svolta dai soggetti pubblici, alla razionalizzazione e miglioramento dei servizi al pubblico volto ad accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge.*

(1) UKUSA è l'acronimo di UK (*United Kingdom*) e USA (*United State American*), è un'alleanza di paesi anglofoni guidata dagli USA e Regno Unito con scopi di spionaggio ed *intelligence*, riconosciuta anche con il nome di *Five Eyes*.

A prescindere dalla sua finalità, è opinione diffusa, ma non supportata da dati scientifici, che la videosorveglianza possa influenzare in positivo la percezione della sicurezza da parte dei cittadini.

È anche importante distinguere fra videosorveglianza "semplice" (senza riconoscimento automatico dei volti) e videosorveglianza "intelligente" (con riconoscimento e tracciamento dei soggetti). Mentre la prima serve a scopo forense (un atto illegale viene compiuto, le registrazioni vengono utilizzate come "testimoni oculari" del fatto), la seconda è molto più pervasiva e può essere usata anche per evincere a priori le *intenzioni* dei soggetti osservati, le loro abitudini, i loro movimenti, le loro relazioni con altri soggetti, quasi sempre *in assenza di mandati giudiziari.*

D'altro canto, c'è la probabilità che questo strumento possa indurre una modifica del naturale comportamento dei cittadini, che sentendosi costantemente osservati, percepiscono lo strumento come intrusivo e minaccioso nei confronti della loro *privacy*.

Per queste motivazioni è importante regolamentare questo strumento e il suo utilizzo, allo scopo di fornire tutele ai cittadini riguardo all'utilizzo delle immagini e delle informazioni estratte dalle immagini stesse.

1.1 Videosorveglianza in Europa e normativa di riferimento

In Europa i sistemi di videosorveglianza sono al pari di qualsiasi altro strumento rivolto alla raccolta, registrazione e al trattamento di dati che identificano fisicamente una persona.

Di conseguenza sia i suddetti sistemi, sia gli attori che li amministrano sono soggetti alle normative in materia di trattamento dei dati.

La normativa anche nello scenario italiano ha subito diverse revisioni dal precedente Codice Privacy (D.lgs. n. 196/2003) fino al nuovo regolamento europeo per il trattamento dei dati GDPR (*General Data Protection Regulation*).

In particolare i sistemi di videosorveglianza sottostanno alle condizioni di liceità del trattamento del dato esposte negli art. 6 e 9 che non fanno distinzione fra operatori pubblici o privati *A differenza del Codice Privacy (D.lgs. n. 196/2003), il nuovo regolamento europeo non contiene la suddivisione tra condizioni di liceità applicabili a soggetti privati e condizioni valide per i soggetti pubblici, come accadeva con il Capo II del Codice Privacy, dove, ad eccezione del settore sanitario, si menzionava l'istituto del consenso quale elemento distintivo tra titolari privati e titolari pubblici* [5].

Tuttavia, l'art. 6, comma E, del GDPR fa riferimento alla necessità di un trattamento del dato per adempiere a pubblico interesse: *il trattamento è necessario*

per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Il GDPR impone anche delle limitazioni sugli attori che trattano prevalentemente quei dati relativi a situazioni particolari: condanne penali, reati o a connesse misure di sicurezza: *Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica*. Quindi secondo il GDPR i dati raccolti dai sistemi di videosorveglianza installati per questioni di pubblica sicurezza devono essere trattati esclusivamente da operatori pubblici. Altro punto da prendere in considerazione, sempre per quanto riguarda le amministrazioni pubbliche, è la figura del DPO sempre sancita dal GDPR negli art. 37, 38 e 39 [6] che è obbligatoria per quanto riguarda il trattamento dei dati svolto da un'autorità pubblica.

In Italia, sia nel Codice Penale sia in quello di Procedura Penale non vengono menzionati i sistemi di videosorveglianza o sistemi di registrazione video come tecnologia a supporto delle indagini, tuttavia l'art. 243 c.p.p., comma 1, dice che: *Quando dispone l'acquisizione di un documento che non deve rimanere segreto, il giudice, a richiesta di chi ne abbia interesse, può autorizzare la cancelleria a rilasciare copia autentica a norma dell'articolo 116,* dove per documento si intende qualsiasi prova che rappresenta fatti, persone o cose mediante fotografia, cinematografia, fonografia o altro.

Quindi le immagini raccolte dai sistemi di videosorveglianza, non essendo scrittura privata, non sono soggette ai fini dell'utilizzazione processuale: *video che riprendono fasi temporalmente antecedenti all'interrogatorio di un testimone o di un sospettato (telecamere nascoste che videoregistrano il comportamento di soggetti poco prima di essere interrogati); a scopo di sorveglianza sono: i video registrati da telecamere costituenti sistemi di controllo di obiettivi sensibili, accessi, zone di interesse militare, luoghi aperti al pubblico (stazioni ferroviarie, stadi, ecc.)* [1].

1.1.1 Livello di conformità alle normative in Europa

La sorveglianza effettuata con sistemi di videosorveglianza è da considerarsi come un meccanismo per la raccolta dei dati personali in via indiretta e quindi è soggetta alle leggi sulla *privacy*.

Nel 2022 è stato condotto un sondaggio condotto da *Federprivacy*(2) col fine

(2) Associazione professionale iscritta presso il Ministero dello Sviluppo Economico ai sensi della Legge 4/2013.

di analizzare lo scenario europeo sul livello di conformità normativa in merito al trattamento dei dati sensibili raccolti da sistemi di videosorveglianza.

La normativa di riferimento è sempre il GDPR in particolare l'art. 13 (dati personali raccolti presso l'interessato: informazioni da fornire), da cui si evince che persone che transitano in una zona posta a sistema di videosorveglianza devono essere sempre informate e l'informativa va collocata prima di entrare nella zona.

Le sanzioni in caso di violazione della normativa in materia di privacy previste dal GDPR sono disciplinate dagli articoli 83 e 84 e possono arrivare fino a 20 milioni di euro, o colpire dal due al quattro per cento del fatturato annuo delle imprese non conformi.

Nell'indagine sopracitata di *Federprivacy* vengono messi a confronto i paesi membri dell'UE per numero di violazioni del GDPR in merito all'utilizzo di sistemi di videosorveglianza.

In figura 2 e 3 viene riportata la classifica delle nazioni con il maggior numero di sanzioni.

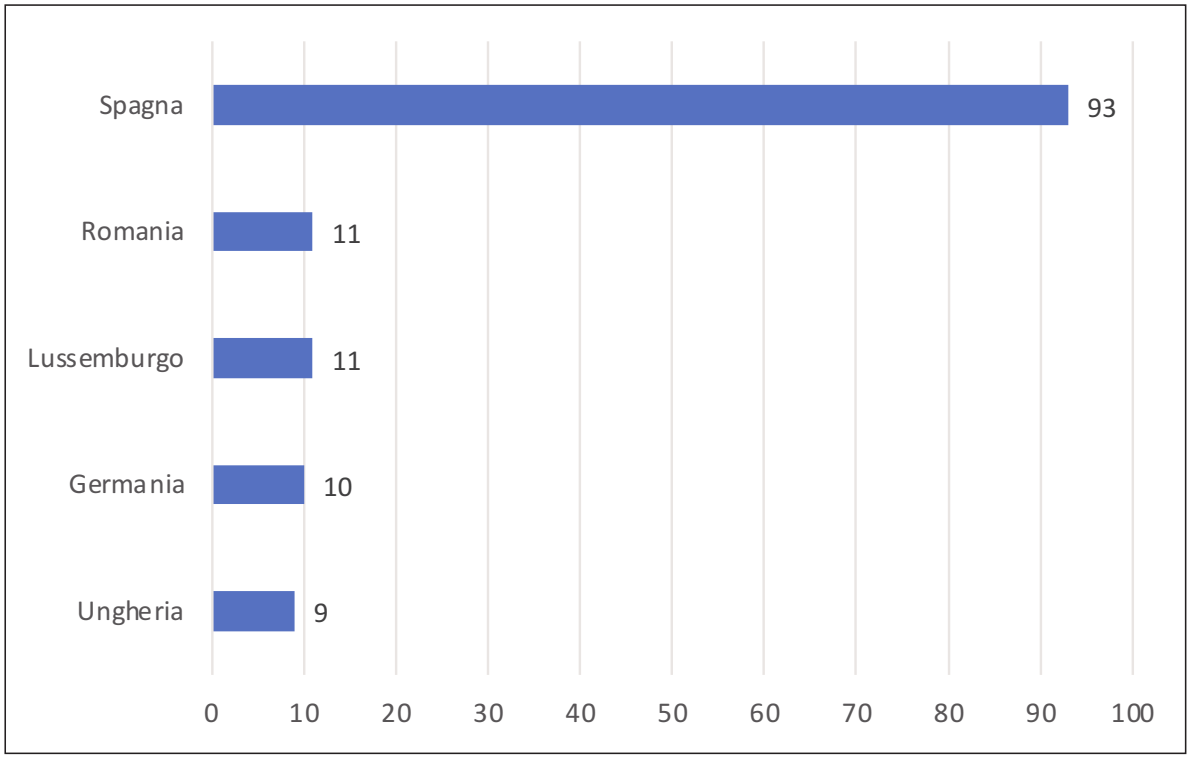

Figura 2: *Nazioni con il maggior numero complessivo di sanzioni per violazioni del GDPR su telecamere e videosorveglianza.*

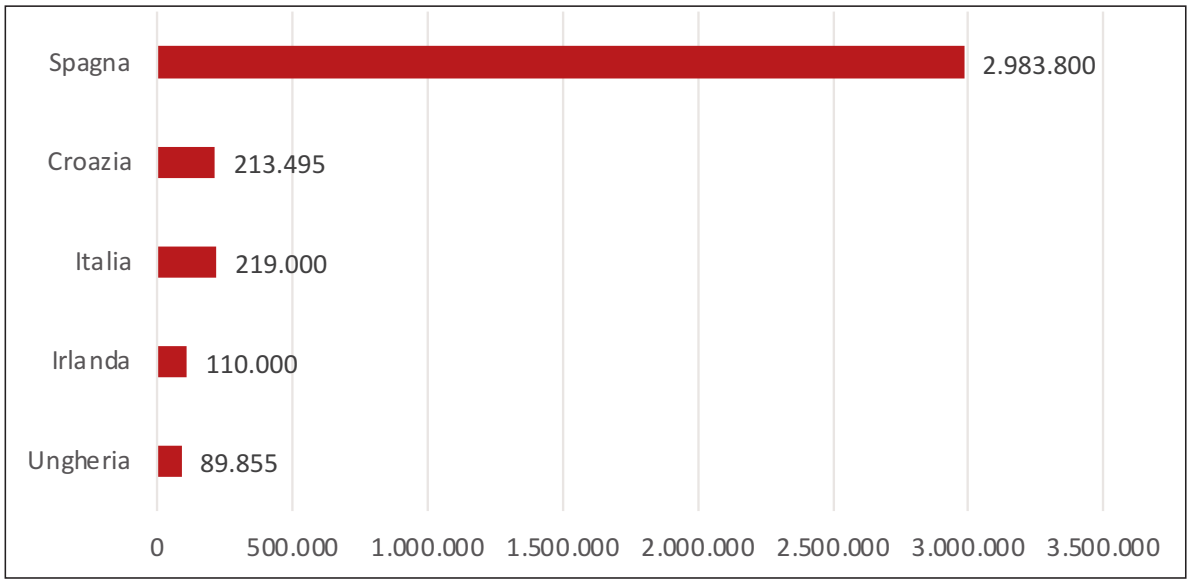

Figura 3: *Nazioni con il maggior valore economico complessivo delle sanzioni (in milioni di €)*

La Spagna risulta in vetta alla classifica sia in termini di numero di sanzioni, sia in termini di valore economico. N.B.: questi dati non evidenziano necessariamente negligenze da parte di chi fruisce del servizio di videosorveglianza o dell'ente preposto AEDP(3), nella corretta applicazione del codice GDPR rispetto agli altri paesi europei. In generale a violare di più le leggi sono le organizzazioni private, con una percentuale di sanzioni pari al 92%.

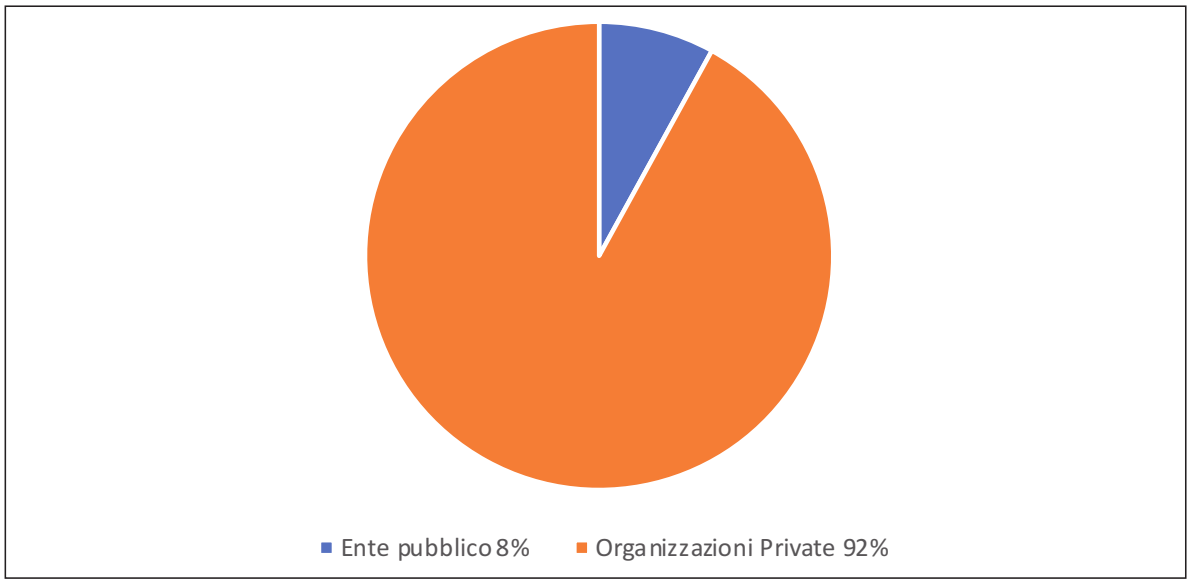

Figura 4: *Percentuali di numero di sanzioni per violazioni del GDPR riguardanti telecamere e videosorveglianza distinte fra pubblico e privato*

(3) AEDP è l'acronimo di *Agencia Española de Protección de Dato* ovvero Agenzia Spagnola per la Protezione dei Dati.

Per quanto riguarda l'Italia, dall'introduzione del GDPR sono pervenute solo 8 sanzioni con importo complessivo pari a 219.000 euro (media di circa 27.000 euro per ogni sanzione). Nella tabella 3 viene riportata la classifica completa delle sanzioni per paese EU.

Nazione	Importo in €	Numero di sanzioni	Importo medio della sanzione in €
Spagna	2983800	93	32084
Lussemburgo	49800	11	4527
Romania	30000	11	2727
Germania	22950	10	2295
Ungheria	89855	9	9984
Grecia	75000	8	9375
Italia	219000	8	27375
Austria	7120	4	1780
Norvegia	66500	4	16625
Belgio	8000	3	2667
Svezia	56200	3	18733
Croazia	213495	2	106748
Polonia	7270	2	3635
Portogallo	4000	2	2000
Bulgaria	1121	1	1121
Finlandia	72000	1	72000
Francia	20000	1	20000
Irlanda	110000	1	110000
Islanda	34000	1	34000
Liechtenstein	4100	1	4100
Repubblica Ceca	2700	1	2700
Cipro	0	0	0
Danimarca	0	0	0
Estonia	0	0	0
Lettonia	0	0	0
Lituania	0	0	0
Malta	0	0	0
Paesi Bassi	0	0	0
Regno Unito*	0	0	0
Slovacchia	0	0	0
Slovenia	0	0	0
** Regno Unito fuori dall'UE dal 2020.*			

Tabella 3: *Elenco delle nazioni europee che hanno irrogato sanzioni per violazioni del GDPR specificatamente riguardanti la videosorveglianza, con i rispettivi dettagli del valore economico complessivo delle sanzioni e il numero dei provvedimenti adottati dall'introduzione del Regolamento UE (da maggio 2018 fino a maggio 2022).*

Si può notare che le sanzioni partono da circa 1.100 euro come nel caso della Bulgaria, fino a superare i 110.000 euro come nel caso dell'Irlanda. Entrambi i paesi hanno subito un'unica sanzione.

1.1.2 Garante per la protezione dei dati personali e videosorveglianza in Italia

In Italia, le amministrazioni comunali che intendono installare sistemi di videosorveglianza devono consultare sia il garante per la protezione dei dati personali, sia la prefettura. Nel gennaio del 2022 sono state emanate le linee guida sul trattamento dei dati personali tramite il *Regolamento 2016/679 - Garante Privacy* [13].

Le linee guida richiedono di segnalare tramite cartelli la presenza della videosorveglianza nelle aree sottoposte alla stessa. Non esiste uno standard per il cartello, però il garante propone un modello semplificato con le seguenti diciture:

- Nome del titolare del trattamento del dato;
- Tempo di conservazione del dato;
- Finalità della videosorveglianza;
- Modalità di accesso ai propri dati personali.

In figura 5 viene riportato l'esempio di modello proposto dal garante per la protezione dei dati personali.

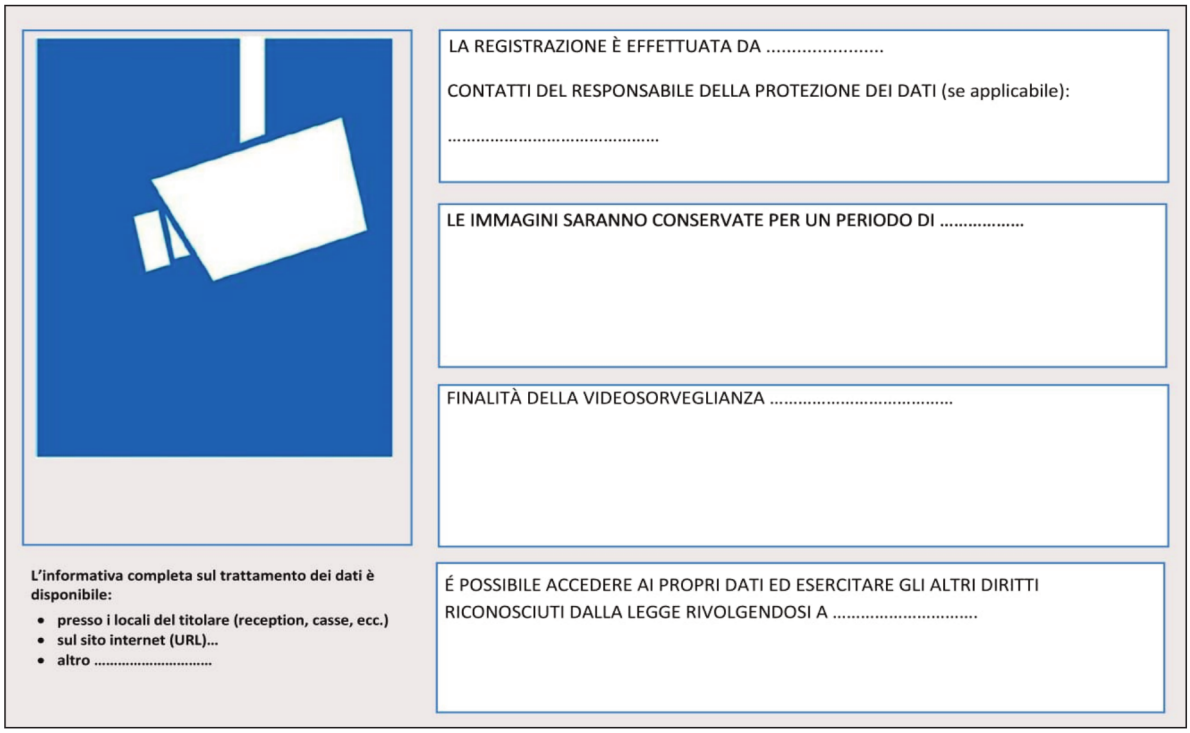

Figura 5: *Modello di cartello proposto da garante per la protezione dei dati personali.*

Sempre il garante per la protezione dei dati personali in Italia ha emanato ulteriori linee guida per l'installazione di sistemi di sorveglianza nell'ambito di attività di carattere personale o domestico, per garantire la sicurezza di persone o beni. Questi sistemi di sorveglianza possono essere installati senza chiedere il parere al garante purché vengano rispettate le seguenti regole:

➢ Le telecamere siano idonee a riprendere *Solo* aree di *Propria Esclusiva Pertinenza*;

➢ Vengano attivate *Misure Tecniche per Oscurare Porzioni di Immagini* in tutti i casi in cui, per tutelare adeguatamente la sicurezza propria o dei propri beni, sia inevitabile riprendere parzialmente anche *Aree* di *Terzi*;

➢ Nei casi in cui sulle aree riprese insista una *Servitù di Passaggio* in capo a terzi, sia acquisito formalmente (una tantum) il *Consenso* del soggetto titolare di tale diritto;

➢ *Non* siano oggetto di ripresa *Aree Condominiali Comuni* o di *Terzi*;

➢ *Non* siano oggetto di ripresa *Aree Aperte al Pubblico* (strade pubbliche o aree di pubblico passaggio);

➢ *Non* siano oggetto di *Comunicazione a Terzi* o di *Diffusione* le immagini riprese.

2 Suddivisione dei ruoli tra Amministrazione locale e Polizia locale

Sul territorio italiano la gestione dei sistemi di videosorveglianza pubblica, insieme a tutte le altre attività relative alla sicurezza urbana, è prevalentemente in capo alle amministrazioni locali, questo perché le competenze degli Enti Locali si sono ampliate notevolmente con il decentramento amministrativo ed il principio di sussidiarietà (legge n. 59/1997; decreto legislativo n. 112/1998 e la legge costituzionale n. 3/2001). Sono quindi cresciute le competenze in ambito sicurezza urbana a livello generale con un coinvolgimento sempre più incisivo e maggiore della Polizia Locale (PL).

Inoltre, anche in caso di emergenza o per organizzare sul territorio i gruppi comunali di protezione civile, la PL rappresenta la struttura operativa che meglio risponde a questo tipo di impiego.

Una fotografia del ruolo degli amministratori locali e della Polizia locale in Italia in termini di sicurezza urbana viene riportata da un'indagine svolta dall'INAPP(4) nel 2020 con riferimento a due fonti:

➢ *ANCI* con il Rapporto nazionale sull'attività della Polizia Locale 2018, relativa all'anno 2017, dell'Associazione nazionale Comuni italiani, con dati forniti dai comandi delle Polizie locali di 157 Comuni, capoluoghi di provincia e non, con popolazione superiore a 50.000 abitanti;

(4) INAPP, Istituto Nazionale per l'Analisi delle Politiche Pubbliche (ex ISFOL).

➢ *FPA-Hexagon*, con una ricerca relativa all'anno 2019, presentata nel corso di Forum PA, *Safe City*. Indagine sulla sicurezza urbana, che fornisce i dati di un campione di 91 Comuni italiani con popolazione superiore ai 20.000 abitanti, raccolti attraverso interviste a sindaci, assessori con delega alla sicurezza, comandanti di Polizia locale di città, tra cui Venezia, Bergamo, Napoli, Genova, Firenze, Parma, Bari. Il dettaglio geografico è il seguente: 29 città capoluogo del Centro e Nord, a cui si aggiungono altre 33 città non capoluogo, 20 città capoluogo del Sud e Isole con ulteriori 9 città non capoluogo.

I risultati dei progetti di ricerca sopra menzionati indicano che nell'80% dei comuni è presente una delega sulla sicurezza urbana. Nella maggior parte dei comuni con presenza di delega, questa è associata alla polizia locale come si evince dalla figura 6 e viene esercitata dal sindaco (nel caso in cui questo sia il capo della PL) oppure da un assessore (nel caso in cui sia esso a capo della PL).

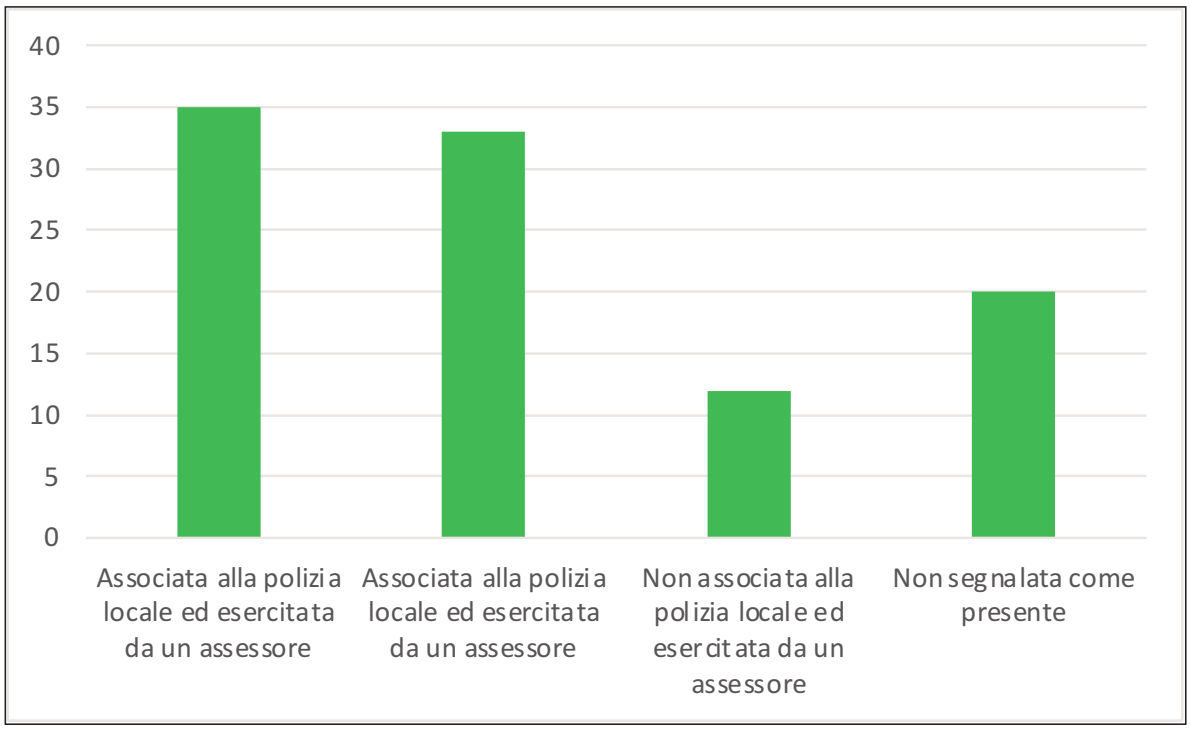

Figura 6: *Presenza della delega alla sicurezza urbana nelle città italiane. Valori espressi in %.*

Sempre secondo l'ANCI, il lavoro svolto dalla PL nel corso del 2017 ha riguardato oltre 280.000 attività operative, di cui il 48,1% sono interventi di sicurezza urbana e di ordine pubblico, il 36,6% riguardano l'identificazione di stranieri e il 15,3% l'attività di polizia giudiziaria. Gli interventi relativi all'ordine pubblico, in occasione di manifestazioni sportive e manifestazioni pubbliche, sono stati 39.137 pari al 13,9% delle attività di polizia di sicurezza.

Dall'indagine in oggetto, in figura 7, si può inoltre evincere che lo strumento riconosciuto come il più efficace nella gestione della sicurezza urbana è la videosorveglianza, tanto che il circa 73% dei comuni propone un ampliamento dei sistemi già in essere. Inoltre, il 27% delle amministrazioni propone di estendere i poteri del sindaco in merito al controllo e gestione della sicurezza urbana.

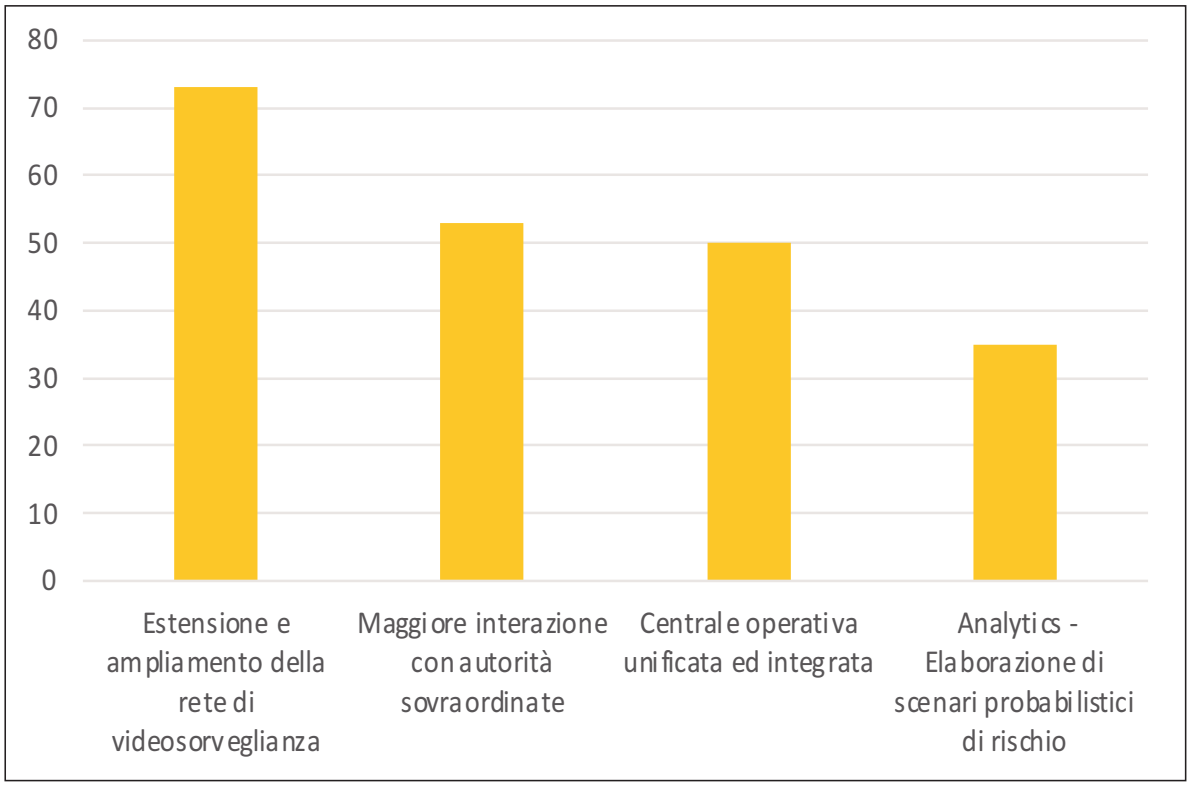

Figura 7: *Settori prioritari di intervento per migliorare la sicurezza urbana. Valori espressi in %.*

La centralità della videosorveglianza era stata ampiamente legittimata, peraltro, anche a livello centrale di governo col Decreto-legge del 20 febbraio 2017, n. 14, Disposizioni urgenti in materia di sicurezza delle città, cosiddetto *Decreto Minniti* dal nome dell'allora ministro dell'Interno.

Il decreto in esame non fa altro che assecondare una tendenza già in atto, anche a livello regionale in materia di sicurezza urbana, promuovendo l'adozione di sistemi di videosorveglianza da parte dei privati cittadini, riconoscendo ai Comuni di deliberare apposite detrazioni sull'imposta municipale (IMU) o sul tributo per i servizi indivisibili (TASI) *in favore dei soggetti che assumono a proprio carico quote degli oneri di investimento, di manutenzione e di gestione dei sistemi tecnologicamente avanzati realizzati in base ad accordi o patti* (articolo 7, comma 1-*bis*) [11].

3 Città italiane videosorvegliate

A pochi mesi dall'entrata in vigore del *Decreto Minniti,* ben 60 città hanno emanato ordinanze al fine di contrastare situazioni di incuria e degrado del territorio e salvaguardare il decoro e la vivibilità in ambito urbano (ANCI 2018, 68). Inoltre, nei 157 Comuni analizzati risultano installate complessivamente 19.015 telecamere di videosorveglianza, in media 122 per ogni città. Le città con il maggior numero di installazioni sono: Roma (3.222 telecamere installate), Milano (2.161) e Trento (520). Analizzando i dati degli ultimi anni si riscontra inoltre un incremento costante dell'indice che mette il numero di telecamere installate a rapporto con il numero di cittadini residenti (telecamere installate ogni 100.000 abitanti). Il valore di quest'indice si attesta a 66 nel 2014, 77 nel 2015, 91 nel 2016, per arrivare a 93 nel 2017 (ANCI 2018, 34).

L'adozione delle videocamere è stata formalizzata in un apposito regolamento presente nel 67,5% dei Comuni italiani (tale valore era di 56,5% nel 2014, di 62,6% nel 2015, di 63,7% nel 2016).

L'insieme delle iniziative attivate dalle amministrazioni locali ha influito positivamente anche sulle condizioni di sicurezza delle città, mentre soltanto il 30% dei comuni intervistati considera che questi interventi abbiano favorito un aumento della percezione della sicurezza urbana da parte dei cittadini, come indicato nella figura 8.

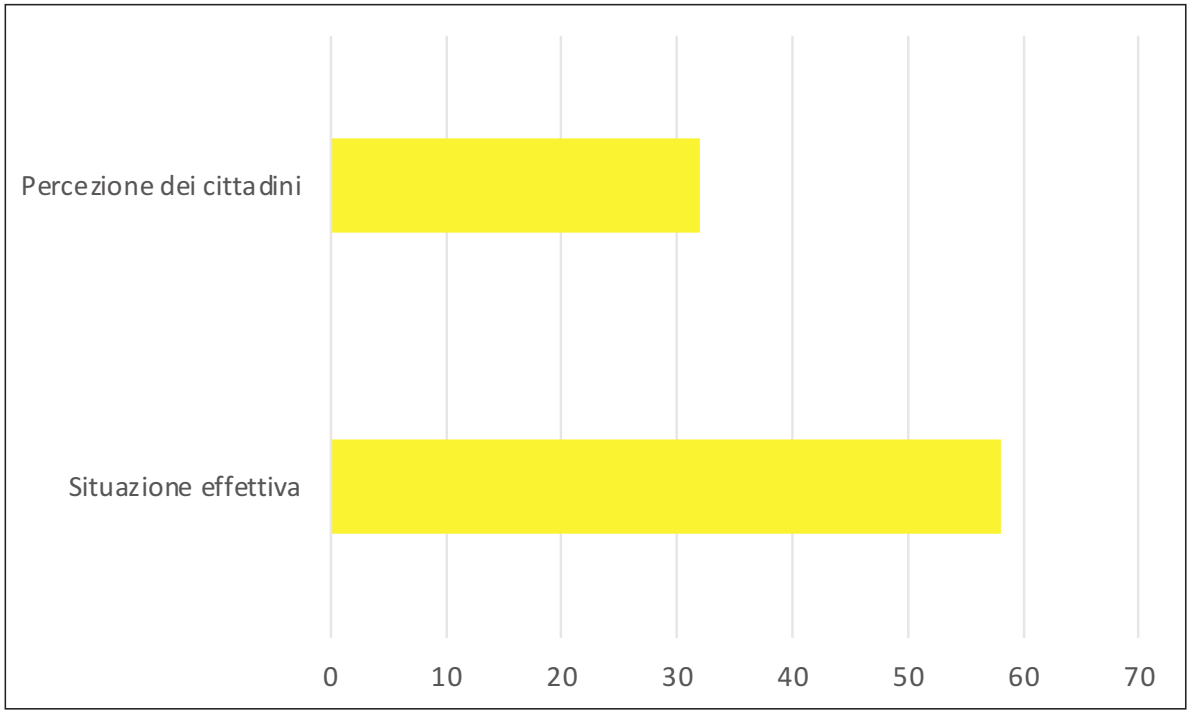

Figura 8: *Miglioramento delle condizioni di sicurezza. Valori espressi in %. Fonte: FPA in esclusiva per Hexagon Safety and Infrastructure, Safe City. Indagine 2019 sulla sicurezza urbana.*

A livello quantitativo ad oggi è difficile dare una stima esatta del numero di dispositivi installati in tutta Italia, poiché è obiettivo di tutti i comuni coprire le aree pubbliche non ancora sottoposte a videosorveglianza. Nonostante ciò, si può affermare che le città più videosorvegliate in Italia sono: *Roma* con 8.300 telecamere e con una media di 1,96 dispositivi per ogni 1.000 abitanti e *Milano* con 4.143 dispositivi e una media pari a 1,32 dispositivi ogni 1.000 abitanti.

4 Confronto fra tecniche di videosorveglianza fra Europa, USA e Cina

Anche gli USA da oltre un ventennio utilizzano la videosorveglianza nei propri comuni per scopi di sicurezza. In questo articolo si fa riferimento ad una specifica città: San Francisco nello stato della California, il cui dipartimento di polizia (SFPD), ha acquistato un sistema di identificazione biometrica automatica (ABIS) nel 2010.

In un sistema di riconoscimento facciale come quello sopra citato, che richiede un addestramento o training, se la *machine learning* alla base viene addestrata con un set di persone di una determinata etnia, allora il riconoscimento facciale sarà più efficiente nell'identificare volti di quell'etnia.

Questo sistema ha quindi da subito mostrato alcuni problemi, non legati alla tecnologia stessa, ma al suo utilizzo: il training supervisionato della *machine learning* è stato svolto prendendo in considerazione molte più persone afroamericane rispetto alle restanti etnie.

Secondo l'ufficio nazionale del censimento americano, *l'US Census*, ad oggi a San Francisco vi sono circa il 5% di afroamericani e il 52% di persone bianche su una popolazione di poco più di 880.000 cittadini residenti nel comune [3].

Gli afroamericani vengono arrestati ad un tasso superiore del 185% rispetto alla loro quota della popolazione cittadina [14], quindi sono dati probabilmente sovra-rappresentati nella elaborazione del training set del *machine learning* di cui sopra;

La polizia si serve di questo sistema per indagini investigative: la polizia può usare il sistema di riconoscimento facciale servendosi di fotogrammi ottenuti da una videocamera di sorveglianza, e confrontandoli con foto scattate da uno smartphone o semplicemente estrapolate dai *social network* di persone indagate.

Negli USA, non è molto chiaro come la Corte Suprema interpreti il primo e il quarto emendamento in merito all'uso di un sistema di riconoscimento facciale tramite telecamere di videosorveglianza.

Il primo emendamento protegge il diritto di riunirsi pacificamente e di inviare petizioni al governo per la riparazione dei torti subiti.

Il quarto emendamento invece sancisce il diritto dei cittadini di godere

della sicurezza personale, della loro casa, dei loro beni, nei confronti di perquisizioni e sequestri ingiustificati; e chiarisce che non si possono emettere mandati giudiziari se non su fondati motivi sostenuti da giuramento o da dichiarazione. Questi emendamenti riportano diverse interpretazioni, spesso anche contraddittorie.

L'uso da parte della polizia del sistema di riconoscimento facciale per identificare continuamente chiunque e senza un sospetto può causare dubbi e perplessità sull'eventuale violazione delle libertà fondamentali di espressione e associazione. In particolare, quando il riconoscimento facciale viene utilizzato da parte delle autorità per la schedatura dei manifestanti durante le manifestazioni pubbliche per proteste.

I ricercatori del *Center of Privacy and Technology* della facoltà di legge dell'Università di Georgetown hanno individuato tre livelli di rischio derivanti dall'uso del sistema di riconoscimento facciale:

➢ *Moderato*: fa riferimento ai metodi classici di raccolta dei dati biometrici dei cittadini.

➢ *Alto*: riguarda l'uso di banche dati di dati biometrici di cittadini senza precedenti.

➢ *Molto Alto*: quando vengono continuamente raccolte informazioni da filmati provenienti da sistemi di videosorveglianza e telecamere corporee indossate dalla polizia che creano problemi per la privacy e le libertà dei cittadini.

Prima della videosorveglianza e del riconoscimento facciale tramite telecamere, i database della polizia erano popolati esclusivamente di dati biometrici presi da criminali, come il database di DNA dell'FBI, che per legge federale, deve essere composto solo da campioni raccolti da persone arrestate o campioni raccolti a seguito di indagini forensi.

Tuttavia, l'FBI con i sistemi di riconoscimento facciale (*FACE Services*) arricchisce il proprio set di informazioni, creando una rete di database composta da dati biometrici anche di altri cittadini. Tali informazioni permettono di creare "grafi sociali" (relazioni fra soggetti/cittadini, abitudini, spostamenti, ecc.) che danno alle agenzie governative un eccessivo potere di indagine a tappeto.

Sembrerebbe che diverse questioni relative all'acquisizione di dati biometrici tramite riconoscimento facciale acquistato dal dipartimento di polizia siano state risolte dal *Consiglio delle autorità di vigilanza di San Francisco*(5) bandendo l'utilizzo della tecnologia di riconoscimento facciale (con un voto di 8 a 1). Quindi San Francisco è di fatto la prima grande città a impedire il suo utilizzo.

(5) Il consiglio delle autorità di vigilanza di San Francisco è l'organo legislativo all'interno del governo della città e della contea di San Francisco, California, Stati Uniti.

Il divieto in particolare proibisce l'utilizzo della tecnologia di riconoscimento facciale o le informazioni raccolte da sistemi esterni che utilizzano la stessa tecnologia.

Fa parte di un più ampio pacchetto legislativo ideato per governare l'uso delle tecnologie di sorveglianza in città, che richiede alle agenzie locali di verificare maggiormente l'uso di questi strumenti.

Mentre la San Francisco *Police Officers Association* ha affermato che il divieto ostacolerebbe gli sforzi degli agenti impiegati per indagare sui crimini, è necessario anche considerare che *La lotta per il riconoscimento facciale a San Francisco è in gran parte teorica: il dipartimento di polizia non utilizza attualmente tale tecnologia. È in uso solo negli aeroporti e porti internazionali che sono soggetti alla giurisdizione federale e non sono interessati dalla legislazione locale* [15].

Per quanto riguarda lo scenario asiatico, in particolare la Cina, la questione videosorveglianza e riconoscimento facciale non risente di grossi impedimenti o limitazioni da parte delle autorità locali in quanto il governo cinese è il primo a promuovere l'impiego e l'utilizzo di nuove tecnologie in merito alla sicurezza nazionale.

Difatti la Cina è la nazione con il maggior numero di città videosorvegliate nel mondo: come riportato da un'indagine della *CNN*, tra le dieci città più sorvegliate al mondo, otto sono in Cina [10], come si vede dalla figura 9.

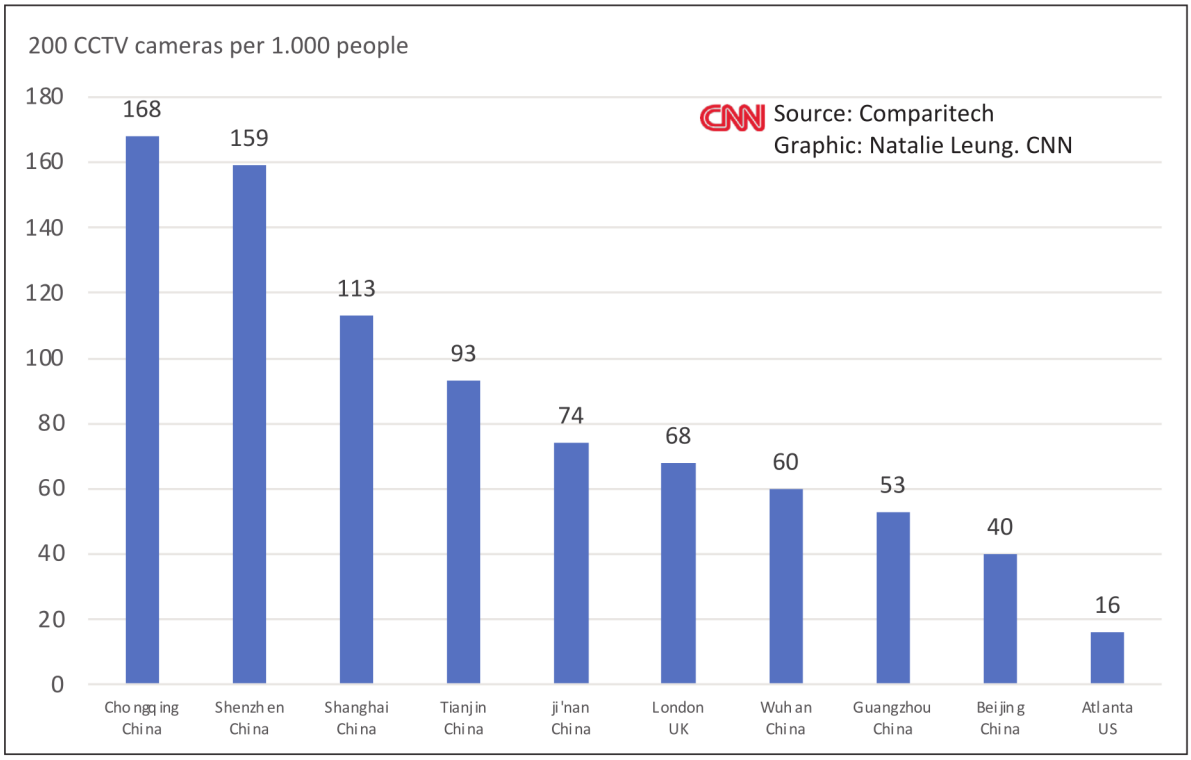

Figura 9: *Città video sorvegliate al mondo.*

A livello globale, la Cina non è solo lo stato con il maggior numero di telecamere installate, ma è anche la "migliore" a livello tecnologico; infatti, la maggior parte delle città cinesi che adottano un sistema di videosorveglianza ha anche un sistema di riconoscimento facciale. In questo caso si parla di città *super sorvegliate*, come Shenzhen. Il sistema di videosorveglianza intelligente di Shenzhen è stato implementato a partire dal 2006, e da allora ha subito diversi perfezionamenti, tra cui l'installazione di un particolare chip che fornisce potenza di calcolo per il riconoscimento delle caratteristiche facciali in loco, e di inviarle in un server *cloud* in grado di elaborare oltre 100 milioni di dati biometrici in meno di un secondo. L'obiettivo di questo sofisticato sistema è di riconoscere in modo automatico con sistemi decisionali-esecutivi eventuali persone ricercate.

Secondo i dati della Polizia di Shenzhen dall'introduzione della *super sorveglianza,* i reati sono diminuiti del 25%, con oltre il 60% di casi risolti grazie alla videosorveglianza [17][9].

5 Conclusioni

In questo articolo partendo dalle *Smart City*, ovvero le città evolute, o che intendono evolversi e diventare *Smart* si è trattato in maniera approfondita di un fattore tecnologico delle città: la videosorveglianza.

Nell'approfondimento sono state evidenziate anche le dovute attenzioni alla tutela dei dati personali, che potrebbero avere un risvolto molto più incisivo soprattutto in ambito sicurezza urbana.

Ciò è particolarmente evidente quando si utilizzano sistemi di videosorveglianza che, seppur implementati con le migliori intenzioni di tutela della sicurezza o per scopi investigativi da parte delle autorità locali, per loro natura sollevano grossi problemi e questioni relative alla tutela dei dati personali.

Questo in quanto i sistemi di videosorveglianza, largamente utilizzati in tutto il mondo, sono in continua evoluzione a livello tecnologico e in alcuni paesi sono dotati anche di riconoscimento facciale. In particolare, in Italia l'impiego di questa tecnologia ha suscitato diverse polemiche, che hanno richiesto l'intervento del ministro dell'Interno.

Il prefetto Piantedosi, attuale titolare del Viminale, si è espresso recentemente [7] tramite la stampa nazionale indicando la videosorveglianza come fondamentale strumento in progressiva estensione (concordata con le autorità locali).

E in particolare con riferimento al riconoscimento facciale ha affermato che può contribuire in maniera ulteriore alla prevenzione e alle indagini.

Tuttavia, nella sua intervista riconosce che è necessario bilanciare in maniera equilibrata il diritto alla sicurezza e il diritto alla privacy dei cittadini.

È importante ricordare quando si parla di riconoscimento facciale che, specie quando applicato da autorità pubbliche nei luoghi pubblici come le stazioni, per esempio, dove transitano migliaia di persone diverse ogni giorno, nello scenario ipotizzato dal ministro, queste verranno sottoposte a una sorveglianza continua, senza mandati giudiziari. Il che significa raccogliere miliardi di dati (di relazione e di abitudini) su tutti i cittadini con gravi implicazioni etiche e morali.

Attualmente esistono già dei riferimenti normativi italiani che tutelano il cittadino sull'uso sconsiderato della tecnologia del riconoscimento facciale biometrico. Il suo impiego per finalità di pubblica sicurezza e indagini penali è consentito infatti dalla normativa vigente (nello specifico, dalla conversione del decreto-legge 139/21) da quasi due anni. Inoltre, la Corte di cassazione non rileva nei luoghi pubblici una ragionevole aspettativa di privacy.

Rimane di fondamentale importanza mantenere la situazione equilibrata tra sicurezza e privacy perché, se da un lato, la sicurezza si può garantire anche tramite controllo diffuso con videosorveglianza, dall'altro l'applicazione di controlli più estesi ed efficaci genera nelle persone una reazione di istintivo rifiuto.

La questione del bilanciamento tra i diritti di sicurezza e privacy finora trattata richiede anche interventi da parte del parlamento EU (Unione Europea) della UE, che poi ogni stato facente parte dell'Unione dovrà recepire in maniera autonoma. La discutibile motivazione fondamentale di un intervento a livello globale europeo è che il superiore interesse degli Stati membri e la tutela della collettività non possano essere limitati "in nome della privacy". È anche vero che esistono già dei meccanismi di tutela del cittadino per evitare che le attività di pubblica sicurezza si traducano in una potenziale limitazione dei diritti.

Attualmente la direttiva 680/16 recepita anche dall'Italia si occupa della questione e fornisce già degli strumenti per controllare, caso per caso, se una specifica attività di polizia connessa alla raccolta di dati e informazioni abbia superato o meno i confini fissati per legge. Ma l'impianto di regole riguardante l'argomento è ancora tutt'oggi oggetto di discussione da parte della stessa EU.

Nel percorso tuttora in essere per la ricerca del delicato equilibrio tra diritto alla sicurezza e diritto alla privacy, con riferimento a queste tecnologie evolute adottate esclusivamente dalle forze dell'ordine, la posizione di fiducia nell'impiego di questi strumenti in nome di una maggiore tutela della sicurezza dei cittadini dovrebbe rappresentare una posizione di fiducia nelle istituzioni.

Riferimenti bibliografici

[1] Giuseppe Delfinis Arma dei Carabinieri Gianfranco De Fulvio. Le indagini video-fotografiche - approccio tecnico e giuridico. http://www.carabinieri.it/editoria/rassegna-dell-arma/la-rassegna/anno-2005/n-2—-aprile-giugno/studi/leindagini-video-fotografiche—-approccio-tecnico-egiuridico.

[2] articolo del wall street jurnal di Stephen Fidler. Echoes of echelon in charges of NSA spying in Europe, 2013.

[3] Unite State Census. https://www.census.gov/quickfacts/sanfranciscocountycalifornia, 2019.

[4] Congresso degli Stati Uniti d'America. Protect American act. https://www.congress.gov/bill/110th-congress/senate-bill/1927, 2007.

[5] di Michele Lasselli Dipendente ente locale PA altalex.com. Gdpr: gli adempimenti a carico dei comuni. https://www.altalex.com/documents /news/2018/04/05/gdprgli-adempimenti-a-carico-dei-comuni, 2018.

[6] Unione Europea. Gdpr. https://eur-lex.europa.eu/legalcontent /IT/TXT/HTML/?uri=CELEX:32016R0679#d1e3729-1-1, 2018. J. Ramon Gil-Garcia, USA Theresa A. Pardoa of the University at Albany, State University of New York, and Korea Taewoo Namc of the Myongji University. What makes a city smart? identifying core components and proposing an integrative and comprehensive conceptualization - information polity 20 (2015) 61–87 61 doi 10.3233/ip-150354 ios press, 2015.

[7] iltempo.it. Piantedosi prepara il riconoscimento facciale: più telecamere nelle stazioni. 2023.

[8] larepubblica.it. Echelon, parla un pentito "non fantascienza ma realtà". https://www.repubblica.it/online/tecnologie_internet/echelon5/spia/spia.html, 2000.

[9] Shenzhen Municipal Public Security Bureau e.huawey.com. Li Shihua, Chief of the Video Police Division. Video big data: Especially useful for public safety. https://e.huawei.com/it/publications/global/ict_insights/201711060837/public/201712280841.

[10] CNN Business Nectar Gan. China is installing surveillance cameras outside people's front doors and sometimes inside their homes. https://edition.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html, 2020.

[11] Achille Pierre Paliotta. Le politiche innovative di sicurezza nelle città tra tecnologie di riconoscimento e smart cities. 2020.

[12] Garante per la protezione dei dati personali. Provvedimento in materia di videosorveglianza. https://www.garanteprivacy.it/documents/10160/10704/Provvedimento+in+materia+di+videosorveglianza+-+leaflet+.pdf/6c3df7ec-7f25-4d5f-9ef9-eaebf6e9f0df?version=1.2, 2020.

[13] Garante per la protezione dei dati personali. Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video versione 2.0. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_it.pd, 2022.

[14] U.S. Census San Francisco Police Department, State of California Department of Justice Office of the Attorney General. Jurisdiction San Francisco. https://www.perpetuallineup.org/jurisdiction/san-francisco, 2016.

[15] Richard Fausset the new york times Kate Conger and Serge F. Kovaleski. San francisco bans facial recognition technology. https://www.nytimes.com/2019/05/14/us/facialrecognition-ban-san-francisco.html, 2019.

[16] Legislation UK. Metropolitan police act 1829. legislation.gov.uk 1829 c. 44 (Regnal. 10Geo4), 1829.

[17] Roberta De Santis Alessandra Fasano Nadia Mignoli Anna Villa. Il fenomeno smart cities - rivista italiana di economia, demografia e statistica. http://www.treccani.it/vocabolario/smart-city_res-72b7b87c-89ec-11e8-a7cb00271042e8d9_%28Neologismi%29/, 2014.