REGIONE PIEMONTE
Quaderni di aggiornamento per la Polizia Locale

QUADERNI PUBBLICATI:

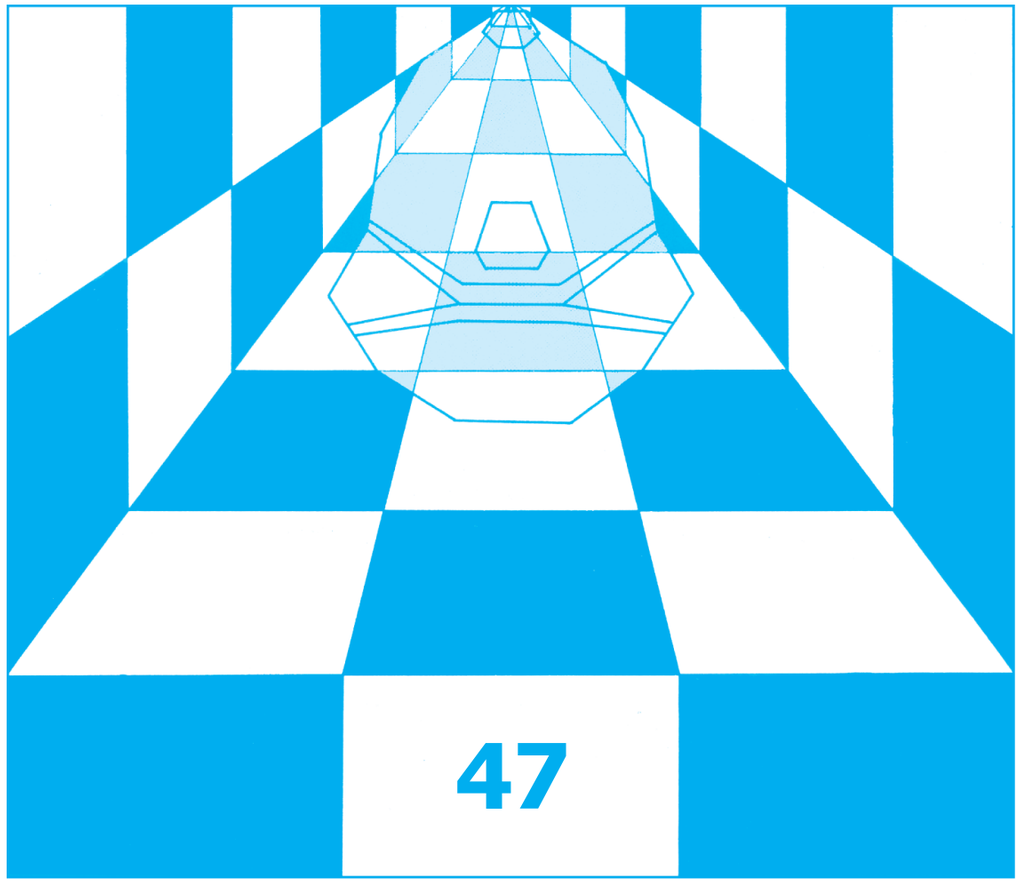
N. **1** - IL COMMERCIO AMBULANTE*
N. **2** - INFORTUNISTICA STRADALE*
N. **3** - LE FUNZIONI DI POLIZIA GIUDIZIARIA*
N. **4** - ETICA PROFESSIONALE E COMPORTAMENTO*
N. **5** - I SEQUESTRI GIUDIZIARI ED AMMINISTRATIVI*
N. **6** - FARE EDUCAZIONE STRADALE*
N. **7** - LEGISLAZIONE E TECNICA DELLE ARMI
N. **8** - DELITTI CONTRO LA PUBBLICA AMMINISTRAZIONE*
N. **9** - VENDITE FALLIMENTARI, SALDI FINE STAGIONE ECC...*
N. **10** - INQUINAMENTI, RIFIUTI, TRASPORTI E DISCARICHE*
N. **11** - EDILIZIA E PREVENZIONE INFORTUNI*
N. **12** - L'ATTIVITA' DI POLIZIA GIUDIZIARIA*
N. **13** - I SEQUESTRI GIUDIZIARI ED AMMINISTRATIVI - Riedizione*
N. **14** - OLTRE L'ADDESTRAMENTO, LA FORMAZIONE - Atti*
N. **15** - NUOVA DISCIPLINA DEGLI STUPEFACENTI - Atti*
N. **16** - LEGISLAZIONE E TECNICA DELLE ARMI - Riedizione*
N. **17** - ETICA PROFESSIONALE E COMPORTAMENTO*
N. **18** - COMMENTO DEL REGOLAMENTO AL C.d.S..*
N. **19** - COMMENTO AL NUOVO C.D.S..
N. **20** - LA RESPONSABILITA' DELL'OPERATORE DI P.M. NELL'AMBITO DELLA P. A.*
N. **21** - IL COMMERCIO SU AREE PUBBLICHE*
N. **22** - INFORTUNISTICA STRADALE*
N. **23** - IL NUOVO PROCEDIMENTO AMMINISTRATIVO*
N. **24** - LA VIGILANZA EDILIZIA ED URBANISTICA NELL'ATTIVITA' DI POLIZIA MUNICIPALE*
N. **25** - LA VIGILANZA AMBIENTALE NELL'ATTIVITA' DI POLIZIA MUNICIPALE*
N. **26** - LA NUOVA NORMATIVA SU IMMIGRAZIONE E STRANIERI: IL RUOLO OPERATIVO DELLA P. M*
N. **27** - IL REGIME SANZIONATORIO DELLE VIOLAZIONI AI REGOLAMENTI LOCALI ED ALLE ORDINANZE COMUNALI*
N. **28** – I NOMADI ED IL RUOLO DELLA P.M. *
N. **29** – IL COMMERCIO AL DETTAGLIO*
N. **30** – MODIFICHE AL TESTO UNICO DI PUBBLICA SICUREZZA E NORMATIVA SULLA TUTELA DEI DIRITTI D'AUTORE*
N. **31** – MACCHINE AGRICOLE E MACCHINE OPERATRICI*
N. **32** – LA VIGILANZA EDILIZIA ED URBANISTICA*
N. **33** – DIZIONARIO DEI TERMINI PIÙ RICORRENTI AD USO DELLA POLIZIA LOCALE*
N. **34** – LA TUTELA DEGLI ANIMALI: PROBLEMATICHE D'INTERESSE DELLA POLIZIA MUNICIPALE*
N. **35** – LA VIGLIANZA AMBIENTALE NELL'ATTIVITÀ DELLA POLIZIA MUNICIPALE*
N. **36** - L'ATTIVITÁ DI NOTIFICAZIONE DEGLI ATTI: FORME, MODALITÁ E TUTELA DELLA RISERVATEZZA*
N. **37** – L'AUTOTRASPORTO MERCI*
N. 38 –COMMENTO AL NUOVO CODICE DELLA STRADA – TITOLI I - II - III (DALL'ART. 1 ALL'ART. 114) PARTE PRIMA*
N. 38 – COMMENTO AL NUOVO CODICE DELLA STRADA – TITOLI IV - V - VI - VII (DALL'ART. 115 ALL'ART. 240) PARTE SECONDA
N. 38 – COMMENTO AL NUOVO CODICE DELLA STRADA – TITOLI IV - V - VI - VII (DALL'ART. 115 ALL'ART. 240) - AGGIORNAMENTO
N. 39 – LA VIGILANZA AMBIENTALE NELL'ATTIVITA' DELLA POLIZIA MUNICIPALE - RIEDIZIONE
N. 40 – LE NOVITA' INTRODOTTE IN MATERIA DI SICUREZZA URBANA
N. 41 – LA VIGILANZA EDILIZIA ED URBANISTICA NELL'ATTIVITA' DELLA P.M. – RIEDIZIONE AGGIORNATA
N. 42 –IL SERVIZIO AUTOMONTATO. PROCEDURE OPERATIVE STANDARD PER IL PERSONALE ADIBITO A FUNZIONI DI POLIZIA STRADALE
N. 43 – COMMENTO AL NUOVO C.D.S. TITOLI II° - IV – V - VI
N. 44 – INFORTUNISTICA STRADALE – RIEDIZIONE AGGIORNATA
N. 45 I CONTROLLI DI POLIZIA SULLA DISCIPLINA DEI VIDEOGIOCHI
N. 46 AUTOPROTEZIONE E PROCEDURE OPERATIVE STANDARD PER GLI OPERATORI DI P.L.

*** copie esaurite**

REGIONE PIEMONTE

Assessorato alla Promozione della Sicurezza e alla Polizia Locale

LA VIDEOSORVEGLIANZA E GLI ENTI LOCALI



Quaderni di aggiornamento per la polizia locale

LA VIDEOSORVEGLIANZA E GLI ENTI LOCALI

n. 47

Quaderni di aggiornamento per la polizia locale

PRESENTAZIONE

Sempre più i sistemi di video sorveglianza sono utilizzati dalle Amministrazioni Locali come strumento di rassicurazione, perché offrono il vantaggio di dare una risposta immediata al senso di insicurezza dei cittadini. Nel sistema complessivo della sicurezza la tecnologia svolge e può svolgere un ruolo molto importante.

Si tratta di dispositivi piuttosto delicati che, per il loro corretto utilizzo sul territorio, devono saper coniugare sia il valore della sicurezza sia quello della privacy, prevedendo anche una specifica manutenzione. Accendendo le telecamere, infatti, gli organi pubblici devono essere consapevoli di perseguire esclusivamente fini istituzionali, rispettando anche i criteri di proporzionalità, di finalità, e di necessità che vincolano giuridicamente gli strumenti della videosorveglianza.

In questo particolare contesto, l'Assessorato regionale alla Sicurezza e Polizia Locale ha recentemente realizzato un censimento rispetto alla diffusione dei sistemi di videosorveglianza di proprietà degli Enti Locali. Ciò al fine di poter disporre di una mappa quantitativa e qualitativa di tali tecnologie, raccogliendo informazioni e spunti di riflessione utili alla valutazione dell'attività di programmazione di interventi in materia di sicurezza integrata.

Marzo 2011

Elena MACCANTI
Assessore Regionale alla Promozione della Sicurezza

LA VIDEOSORVEGLIANZA NEGLI ENTI LOCALI

Premessa

Dal punto di vista normativo la videosorveglianza è un'attività lecita: lo si desume dall'art. **615 bis c.p**. che punisce l'indebita acquisizione d'immagini mediante l'uso di strumenti di ripresa visiva nell'abitazione altrui o in altro luogo di privata dimora, con l'ovvia conseguenza che è consentito acquisire immagini in luogo pubblico o aperto al pubblico.

I sistemi di videosorveglianza che vengono installati da soggetti pubblici o privati hanno la finalità di contenere i fenomeni criminali, sia attraverso il meccanismo della repressione - se avviene una rapina in una zona ove sono presenti telecamere può risultare più facile attraverso questo strumento individuare i responsabili - sia attraverso quello che è il meccanismo della prevenzione sotto la forma della deterrenza.

Prevenire il crimine oppure reprimerlo attraverso la videosorveglianza comporta però un problema di bilanciamento tra contrapposti interessi, quello della sicurezza pubblica e quello della riservatezza della persona.

L'art. 134 [1] del Codice della Privacy, nel prevedere che il garante promuova la sottoscrizione di un codice deontologico e buona condotta, definisce videosorveglianza *"il trattamento effettuato con strumenti elettronici di rilevamento immagini"*.

Tale definizione, ben lungi dall'essere esaustiva, va integrata dai numerosi casi sottoposti all'esame dell'autorità attraverso reclami, segnalazioni e richieste di parere, i quali evidenziano un utilizzo crescente spesso non conforme alla legge, *"di apparecchiature audiovisive che rilevano in modo continuativo immagini, eventualmente associate a suoni, relative a persone identificabili, spesso anche con registrazione e conservazione di dati."*

Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza non forma oggetto di legislazione specifica, ma si applicano al riguardo le disposizioni generali in tema di protezione dei dati personali.

Il Codice in materia di protezione dei dati personali - D. Lgs 196 del 30.6.2003 - tutela il diritto alla riservatezza, diritto costituzionalmente garantito e l'installazione di sistemi, reti ed apparecchiature che permettono la ripresa e l'eventuale registrazione di immagini rappresenta una delle modalità con cui vengono trattati dati personali.

Il Garante della Privacy ha poi provveduto a dettare regole per disciplinare nello specifico l'installazione di impianti di videosorveglianza: l'interferenza nella vita privata altrui attraverso le telecamere trova così nei provvedimenti dell'Autorità un deterrente.

E' doveroso peraltro sottolineare che l'intento del Garante non è quello di evitare la proliferazione dei sistemi di videosorveglianza, ma semplicemente la regolamentazione nell'utilizzazione dei sistemi di videosorveglianza, considerato che l'esigenza di tutela della sicurezza è un diritto sempre più sentito a livello di opinione pubblica tanto quanto è sentito il diritto alla riservatezza.

[1] *Art. 134. del Codice della Privacy - Codice di deontologia e di buona condotta*

Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini, prevedendo specifiche modalità di trattamento e forme semplificate di informativa all'interessato per garantire la liceità e la correttezza anche in riferimento a quanto previsto dall'articolo 11

CAPITOLO I – IL TRATTAMENTO DEI DATI PERSONALI MEDIANTE VIDEOSORVEGLIANZA

1. Evoluzione normativa

In questo quadro il Garante per la protezione dei dati personali, in attesa di dare esecuzione al disposto dell'art. 134 del Codice della Privacy che prevede l'emanazione di un codice deontologico sulla videosorveglianza, sollecitato da numerose richieste in merito alle cautele necessarie per conformare alla allora vigente normativa (L. 675/96), gli impianti di videosorveglianza stabili o comunque non occasionali, installati in particolare a fini di sicurezza, di tutela del patrimonio, di controllo di determinate aree e di monitoraggio del traffico o degli accessi di veicoli nei centri storici, aveva dettato regole da rispettare da parte di chi decide di installare ed utilizzare un sistema di videosorveglianza, emanando "**Il decalogo delle regole per non violare la privacy - 29 novembre 2000"** indicante gli adempimenti, le garanzie e le tutele necessarie in base ai principi della legge sulla protezione dei dati personali.

Successivamente, con l'intento soprattutto di aggiornare le regole in materia di videosorveglianza a quanto previsto dal nuovo Codice della Privacy (D. lgs 196/2003), che come noto ha abrogato la legge 675/96 sostituendola, il Garante ha elaborato il " **provvedimento generale sulla videosorveglianza emesso in data 29.4.2004"** contenente una disciplina più compiuta ed organica, con la precisazione dei **principi e degli adempimenti** che devono essere posti in essere dal titolare del trattamento che effettua la videosorveglianza.

2. I principi della videosorveglianza

I principi di liceità, proporzionalità, necessità e finalità .

2.1 Principio di Liceità

Il trattamento di dati raccolti attraverso un sistema di videosorveglianza è possibile solo se fondato su uno dei presupposti di legalità previsti dal Codice della Privacy e deve essere effettuato nel rispetto delle prescrizioni stabilite dalla normativa in materia di protezione di dati personali, ovvero nello svolgimento di funzioni istituzionali riguardo agli enti pubblici e nel cosiddetto "bilanciamento degli interessi" per quanto riguarda soggetti privati ed enti pubblici economici.

Ciò significa che l'ente pubblico per perseguire le sue finalità con la videosorveglianza è comunque soggetta a tutti gli altri adempimenti previsti dalla legge eccetto che richiedere la manifestazione del consenso da parte degli interessati.

Viceversa, quando l'ente pubblico non agisce per fini istituzionali, ma ad esempio per autotutela, è soggetto alle medesime regole imposte ai privati operando nei confronti dei terzi interessati come un normale soggetto di diritto privato.

Vanno inoltre rispettate tutte le altre disposizioni dettate dalle vigenti leggi penali e civili (es. interferenza illecita nella vita privata, statuto dei lavoratori, ecc.).

I presupposti di liceità indicati dal Garante, si differenziano a seconda del soggetto titolare del trattamento dei dati:

a) Sistemi di videosorveglianza utilizzati da persone fisiche

Nel provvedimento del 29.4.2004 sulla videosorveglianza il Garante ha precisato che nell'uso delle apparecchiature volte a riprendere aree esterne ad edifici (perimetrali di muri e recinti, parcheggi, zone carico e scarico, accessi, uscite d'emergenza) il trattamento deve essere effettuato avendo cura di **limitare l'angolo di visuale alla sola area da proteggere**, evitando di riprendere i luoghi circostanti o non rilevanti.

Al fine di evitare di incorrere nel reato di cui all'art. 615 bis del Codice Penale, l'installazione di sistemi di videosorveglianza in immobili privati, all'interno di condomini e loro pertinenze (box, posti auto), sebbene non soggetta alle disposizioni del Codice della Privacy, deve essere effettuata con cautele per salvaguardare diritti dei terzi.

L'angolo di visuale deve essere rigorosamente limitato agli spazi che necessitano di videosorveglianza e che comunque sono di pertinenza, **rimanendo esclusa la possibilità di riprendere** (anche senza registrazione) **cortili, pianerottoli, scale o garage comuni**. Quando si tratta di telecamere che, anche per breve tempo, riprendono pianerottoli o porzioni di scale al passaggio di persone o cose, esse devono essere segnalate con idonea informativa.

Trova piena applicazione il Codice della Privacy se la ripresa di aree condominiali viene effettuata da più proprietari o condomini, oppure dall'amministrazione del condominio.

In ogni caso l'installazione e l'utilizzo di sistemi di videosorveglianza è lecita solo se è riscontrabile un'effettiva esigenza di prevenzione da situazioni concrete di pericolo, di regola costituite da illeciti verificatisi in precedenza, ovvero laddove vi siano attività che comportano la custodia di danaro o valori.

b) Sistema di videosorveglianza installato da persona giuridica

L'art. 23 del Codice della Privacy stabilisce che il trattamento di dati personali da parte di privati o enti pubblici economici è ammesso solo con il consenso espresso dell'interessato ovvero se si rientra in uno dei casi indicati dall'art. 24 del Codice.

Tra i casi espressamente indicati dal legislatore rilevano, ai fini della videosorveglianza, i trattamenti di dati e quindi la raccolta d'immagini da parte di soggetti effettuati con un sistema di videosorveglianza:

- per l'adempimento di un obbligo di legge;

- con il libero ed espresso consenso dell'interessato;

- con "bilanciamento degli interessi".

Ciò significa in sostanza che o vi è una norma oppure un regolamento che impone ed autorizza l'utilizzo del sistema di videosorveglianza ovvero in difetto è necessario generalmente reperire il consenso da parte dell'interessato.

Peraltro il Garante si è reso conto che: "*In caso di impiego di strumenti di videosorveglianza da parte di privati ed enti pubblici economici, la possibilità di raccogliere lecitamente il consenso può risultare, in concreto, fortemente limitata dalle caratteristiche e dalle modalità di funzionamento dei sistemi di rilevazione, i quali riguardano spesso una cerchia non circoscritta di persone che non è agevole o non è possibile contattare prima del trattamento. Ciò anche in relazione a finalità (ad es. di sicurezza o di deterrenza) che non si conciliano con richieste di esplicita accettazione da chi intende accedere a determinati luoghi o usufruire di taluni servizi*"

Per tale motivo il Garante ha inteso **regolamentare l'istituto del bilanciamento degli interessi**, che trova la sua formulazione alla lettera g) dell'art. 24 del Codice della Privacy ed attuazione nel provvedimento sulla videosorveglianza 29.4.04

Infatti, il Garante specifica che la rilevazione delle immagini può avvenire senza consenso dell'interessato qualora vengano rispettati tutti gli adempimenti imposti dal provvedimento generale sulla videosorveglianza e la stessa videosorveglianza "*sia effettuata nell'intento di perseguire un legittimo interesse del titolare o di un terzo attraverso mezzi di prova o perseguendo fini di:*

- tutela delle persone o di beni rispetto a possibili aggressioni, furti, rapine,

danneggiamenti, atti di vandalismo;

- finalità di prevenzione incendi;

- finalità di sicurezza del lavoro".

Si tratta di un ragionamento teso a giustificare da un punto di vista giuridico il fatto che, in determinate circostanze pratiche, non è possibile reperire in via anticipata il consenso dal soggetto interessato al trattamento dei suoi dati: ***Si pensi all'ipotesi di un sistema di videosorveglianza installato in una farmacia***

Senza l'istituto del bilanciamento degli interessi qui in esame, sarebbe sempre necessario chiedere il consenso al trattamento (la ripresa o la registrazione delle immagini) a tutti i soggetti che entrano nella farmacia; a quelli che negano il consenso, bisognerebbe quindi impedire di entrare ovvero bisognerebbe fare in modo che non vengano ripresi !

Essendo questa un'ipotesi tutt'altro che praticabile, giustamente il Garante rileva che, se vi è un legittimo interesse da proteggere (pericolo di rapina) si ritiene **non** necessario il preventivo consenso dell'interessato in quanto l'interesse tutelato attraverso la videosorveglianza viene ritenuto equivalente con il diritto alla riservatezza di quel soggetto che potrà essere ripreso dal sistema di videosorveglianza, anche senza il suo consenso.

L'operatività dell'istituto del bilanciamento degli interessi è in ogni caso strettamente correlata allo scrupoloso adempimento degli oneri previsti per chi utilizza sistemi di videosorveglianza.

c) Sistema di videosorveglianza installato da soggetti pubblici

Il Codice della privacy e le precisazioni del garante fissano alcuni principi fondamentali:

"*Un soggetto pubblico può effettuare attività di videosorveglianza solo ed* ***esclusivamente per svolgere funzioni istituzionali*** (art. 18-22 del Codice della Privacy) *che deve individuare ed esplicitare con esattezza e di cui sia realmente titolare in base all'ordinamento di riferimento.*

Diversamente, il trattamento dei dati non è lecito, anche se l'ente designa esponenti delle forze dell'ordine in qualità di responsabili del trattamento, oppure utilizza un collegamento telematico in violazione del Codice".

Non è quindi lecito, nemmeno per un soggetto pubblico, procedere ad una videosorveglianza capillare di intere aree cittadine, riprese integralmente e costantemente e senza adeguate esigenze..

Risulta parimenti priva di giustificazione l'installazione di impianti di videosorveglianza al solo fine di controllare il rispetto del divieto di fumare o di raccolta di deiezioni canine, di gettare mozziconi o di calpestare aiuole

Contrariamente a quanto prospettato da alcuni enti locali, l'informativa agli interessati deve essere fornita nei termini illustrati dal provvedimento sulla videosorveglianza e non solo mediante pubblicazione sull'albo dell'ente o attraverso una temporanea affissione di manifesti.

Tali soluzioni possono concorrere ad assicurare trasparenza in materia, ma non sono di per sé sufficienti per l'informativa che deve aver luogo nei punti e nelle aree in cui si svolge la videosorveglianza.

Il Garante specifica che: "*Benché effettuata per la cura di un interesse pubblico, la videosorveglianza deve rispettare i principi già richiamati*".

2.2 Principio di Necessità

Il principio di necessità afferma che il trattamento del dato non deve mai superare il limite necessario per il raggiungimento dello scopo prefisso. I sistemi di videosorveglianza possono riprendere persone identificabili **solo se**, per raggiungere gli scopi prefissati, **non possono essere utilizzati dati anonimi**.

Innanzitutto il Garante, richiamando il fatto che la sola presenza di telecamere comporta una influenza nel comportamento delle persone, rimarca il fatto che ciascun sistema informativo e il relativo programma informatico vanno conformati già in origine in modo da non utilizzare dati di persone identificabili quanto sono sufficienti dati anonimi, inoltre il Garante stabilisce che il software va configurato in modo che periodicamente i dati registrati vengano cancellati automaticamente e le immagini registrate possono essere conservate solo per poche ore, al massimo per le 24 ore successive all'acquisizione, fatte salve speciali esigenze di ulteriore conservazione**.**

Degli esempi: se lo scopo della videosorveglianza è quello di monitorare il traffico non saranno consentite zoomate sulle targhe dei veicoli, se al contrario lo scopo è quello di accertare delle violazioni al codice della strada si dovrà zoomare sulle targhe ma non si potranno acquisire immagini relative agli occupanti dell'auto, inoltre la registrazione delle immagini dovrà essere cancellata periodicamente ed automaticamente il più rapidamente possibile

In un esercizio commerciale si rileva la necessità di monitorare una parte del locale aperta al pubblico con un sistema di videosorveglianza poiché, in quella zona, i furti avvengono costantemente nonostante l'installazione di un impianto antitaccheggio. In base al principio di necessità il sistema potrà riprendere soggetti identificabili (la finalità è di protezione dei beni rispetto a possibili furti per cui è necessario poter individuare il malfattore) ma certamente la registrazione delle immagini dovrà essere di breve durata e la cancellazione avvenire in modo automatico per sovraregistrazione. Se quel medesimo sistema venisse installato solo per monitorare l'eventuale sovraffollamento di una data area certamente le riprese non potrebbero riguardare dati identificabili dei soggetti.

2.3 Principio di Proporzionalità

Il principio di proporzionalità afferma che la videosorveglianza deve costituire l'estrema ratio, utilizzabile solo laddove altri sistemi quali allarmi, controlli da parte degli addetti, misure di protezione degli ingressi ecc., risultino insufficienti. Oltre a ciò dovrà essere evitata l'acquisizione di dati in aree che non sono soggette a concreto pericolo, i dati non devono essere eccedenti rispetto alle finalità e devono essere conservati solo per il tempo necessario in relazione ai quali sono raccolti e trattati. Inoltre non giustifica il ricorso alla videosorveglianza il minor costo rispetto ad altre misure di controllo.

E' da escludere quindi la videosorveglianza in aree che non sono soggette a pericolo, con particolare riferimento a quei sistemi installati a mero fine di prestigio; la videosorveglianza è lecita solo se è rispettato questo principio

Procedendo ad una analisi dettagliata è necessario evidenziare i seguenti precetti:

- Si deve evitare la rilevazione di dati in aree che non sono soggette a concreti pericoli o per le quali non ricorre un'effettiva esigenza di deterrenza (esempio tipico sono le telecamere che vengono installate per meri fini di apparenza o di "prestigio")

- Prima d'installare un sistema di videosorveglianza è necessario valutare che altre misure sono da considerarsi insufficienti o inattuabili, in sostanza la videosorveglianza dovrebbe essere l***'extrema ratio*****.**

Su questo precetto il Garante precisa che se la finalità della videosorveglianza è volta alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi d'allarme e ***non deve essere adottata la scelta semplicemente meno costosa, o meno complicata, la quale però potrebbe non tener conto dell'impatto sui diritti degli altri cittadini***

E' vietato l'uso di telecamere a fini promozionali - turistici o pubblicitari, evidenziandosi che la videosorveglianza è ammessa solo se rivolta al controllo di eventi, situazioni o avvenimenti. In sostanza una videocamera che riprende una determinata località e invia tale immagine direttamente in un sito web non è ammissibile se attraverso *web cam* o *cameras-on-line* si rendono identificabili ad un pubblico aperto i soggetti ripresi.

L'indicazione della presenza delle telecamere deve essere fatta attraverso l'informativa e non attraverso la proiezione al pubblico delle immagini riprese. Cioè la finalità del sistema di videosorveglianza non può essere perseguita diffondendo le riprese ad un numero indeterminato di soggetti. In difetto viene leso senz'altro il principio di proporzionalità e probabilmente distorto quello di finalità, con possibili gravi conseguenze circa la liceità delle immagini eventualmente raccolte.

2.4 Principio di Finalità

In base a questo principio il titolare del trattamento può perseguire con la videosorveglianza solo finalità di sua pertinenza, esclusivamente per scopi determinati, espliciti e legittimi. Il titolare può perseguire solo finalità di sua pertinenza, cioè un privato cittadino può installare telecamere per la videosorveglianza della sua proprietà ma non per finalità di sicurezza pubblica e di prevenzione dei reati

Le finalità prefisse devono essere esplicitate, cioè predeterminate e documentate in forma scritta con un atto che deve essere conservato presso il responsabile del trattamento. Devono inoltre essere designate per iscritto tutte le persone fisiche incaricate del trattamento ed autorizzate ad utilizzare gli impianti e, nei casi in cui è indispensabile per gli scopi perseguiti, a visionare le registrazioni. Nel far ciò il Garante raccomanda che ci si deve limitare ad un numero molto ristretto di soggetti.

In ogni caso possono essere perseguite solo le finalità comunicate attraverso l'informativa, ossia direttamente conoscibili attraverso comunicazioni e/o cartelli di avvertimento al pubblico (fatta salva l'eventuale attività di acquisizione di dati disposta da organi giudiziari o di polizia giudiziaria), e **non finalità generiche o indeterminate**, tanto più quando esse siano incompatibili con gli scopi che vanno esplicitamente dichiarati e legittimamente perseguiti.

3. Dal provvedimento generale del garante del 29.4.2004 al provvedimento del 8.4.2010

Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza non forma oggetto di legislazione specifica, ma si applicano al riguardo le disposizioni generali in tema di protezione dei dati personali, integrate dalle disposizioni dettate dal Garante della Privacy.

In considerazione dei numerosi interventi legislativi in materia, sia dell'ingente quantità di quesiti, segnalazioni , reclami e richieste di verifica preliminare in materia sottoposti all'Autorità, il Garante ha ritenuto necessario intervenire nuovamente in tema di videosorveglianza, adottando **il nuovo provvedimento generale dell'8.4.2010**, che sostituisce quello del 2004, introducendo importanti novità.

Questo provvedimento si è reso necessario da un lato per il proliferare negli ultimi anni dei sistemi di videosorveglianza per diverse finalità (prevenzione, accertamento e repressione dei reati, sicurezza pubblica, tutela della proprietà privata, controllo stradale, etc.) e dall'altro in considerazione dei numerosi interventi legislativi adottati in materia - tra questi, quelli più recenti che hanno attribuito ai sindaci e ai comuni specifiche competenze in materia di incolumità pubblica e di sicurezza urbana, così come le norme, anche regionali, che hanno incentivato l'uso di tali sistemi di controllo.

Le importanti novelle sulla videosorveglianza sono contenute nel combinato disposto del **D.L. n. 92/08** (convertito nella L. 24 luglio 2008 n. 125) e del **D.L. 11/09**, (convertito nella L. 23 aprile 2009, n. 38)

Con il pacchetto sicurezza adottato con il D.L**.** 92/2008, che ha riformulato l'art. 54 del T.U.E.L,. il legislatore ha attribuito ai sindaci il compito di sovrintendere alla vigilanza su tutto ciò che possa interessare la sicurezza e l'ordine pubblico e di adottare gli atti loro attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica, nonché svolgere le funzioni affidate ad essi dalla legge in materia di sicurezza e di polizia giudiziaria.

Con la modifica dell'art. 54 il Sindaco, al fine di prevenire e contrastare determinati pericoli che minacciano l'incolumità pubblica e la sicurezza urbana, può adottare con atto motivato provvedimenti, "anche contingibili e urgenti" nel rispetto dei principi generali dell'ordinamento. La nuova formulazione lascia spazio quindi ad un uso ordinario delle ordinanze, quale strumento non necessariamente adottato per motivi di necessità ed urgenza e dotato del carattere della temporaneità

Il D.L. 11/09 in materia di sicurezza pubblica, di contrasto alla violenza sessuale ed atti persecutori, ha poi introdotto all'art. 6/ 7° e 8° comma, la facoltà in capo ai Comuni di utilizzare, per finalità di tutela della sicurezza urbana, sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico; i dati, le informazioni e le immagini raccolte mediante l'uso di detti sistemi sono conservati per sette giorni, ***"fatte salve speciali esigenze di ulteriore conservazione".***

Sino ad allora alcuni comuni italiani si erano serviti di sistemi di videosorveglianza per la tutela della sicurezza urbana, però l'installazione era preceduta dalla stipula di protocolli d'intesa tra sindaci e prefetti, essendo questi ultimi i soli referenti istituzionali in materia di sicurezza pubblica nella Provincia. D'altra parte il codice sulla privacy prevede che qualunque trattamento di dati personali -quindi anche d'immagini- da parte di soggetti pubblici è consentito soltanto nello svolgimento delle funzioni istituzionali e pertanto non rientrando la sicurezza pubblica nella funzione istituzionale dei comuni si riteneva che fossero necessari dei protocolli d'intesa con il Prefetto. In buona sostanza la legittimità delle riprese effettuate dalla polizia municipale era sempre stata collegata alle finalità tradizionali dei comuni ovvero il controllo del traffico, la prevenzione degli atti vandalici in determinate zone, ma mai attività di indagine e di tutela della sicurezza urbana.

Con i recenti interventi legislativi in pratica che attribuiscono al sindaco nuovi poteri in materia di incolumità pubblica e sicurezza urbana, il legislatore ha ammesso la partecipazione diretta dei comuni a questioni prima riservate a polizia e carabinieri.

Con il dm 5 agosto 2008, il Ministro dell'interno ha definito specificamente anche cosa si intende per sicurezza urbana, ovvero "*un bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani"*.

Per effetto di tali definizioni, il sindaco può intervenire per prevenire e contrastare:

a) le situazioni urbane di degrado che favoriscono l'insorgere di fenomeni criminosi, quali lo spaccio di stupefacenti, lo sfruttamento della prostituzione, l'accattonaggio con impiego di minori e disabili e i fenomeni di violenza legati anche all'abuso di alcool;

b) il danneggiamento del patrimonio pubblico e privato con conseguenze non solo economiche, ma che determinano lo scadimento della qualità urbana;

c) fenomeni di abusivismo commerciale e di illecita occupazione di suolo pubblico;

d) schiamazzi o comportamenti che possono turbare gravemente la quiete pubblica o il libero utilizzo degli spazi pubblici o la fruizione cui sono destinati

Riconoscere ai comuni la possibilità di utilizzare la videosorveglianza per la tutela della sicurezza urbana equivale ad assimilare gli impianti tecnici in disponibilità ai comuni a quelli in uso da polizia e carabinieri.

Ciò significa innanzitutto la possibilità di utilizzare immagini ad alta definizione, ma anche la possibilità di conservare i dati registrati per un lasso di tempo ragionevole in relazione alle possibili implicazioni giudiziarie derivanti dalla videoregistrazione. Resta però necessario, per i comuni, assolvere a tutte le complesse burocrazie in materia di videoregistrazione previste solo per loro dal codice privacy.

Il Garante ricorda in premessa nel suo provvedimento che la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali (*art. 4, comma 1, lett. b), del Codice*). ed è considerato dato personale qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

L'utilizzo della videosorveglianza sia per la protezione e l'incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, la protezione della proprietà, rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, o l'acquisizione di prove è possibile purché ciò non determini un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli interessati.

L'installazione di sistemi di rilevazione delle immagini deve però avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, quali ad es. le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata sul controllo a distanza dei lavoratori in materia di sicurezza presso stadi e impianti sportivi, o con riferimento a musei, biblioteche statali e archivi di Stato in relazione ad impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali e, ancora, nell'ambito dei porti, delle stazioni ferroviarie, delle stazioni delle ferrovie metropolitane e nell'ambito delle linee di trasporto urbano

In tale quadro, pertanto, è necessario che:

a) il trattamento dei dati attraverso sistemi di videosorveglianza sia fondato su uno dei presupposti di ***liceità*** che il Codice prevede espressamente per i soggetti pubblici, cioè lo svolgimento di funzioni istituzionali

b) ciascun sistema informativo ed il relativo programma informatico vengano conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (es., configurando il programma informatico in modo da consentire, per monitorare il traffico, solo riprese generali che escludano la possibilità di ingrandire le immagini e rendere identificabili le persone). Lo impone il ***principio di necessità***, il quale comporta un obbligo di attenta configurazione di sistemi informativi e di programmi informatici per ridurre al minimo l'utilizzazione di dati personali

c) l'attività di videosorveglianza venga effettuata nel rispetto del c.d. principio di ***proporzionalità*** nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite

4. L'informativa

Uno degli aspetti più salienti del nuovo provvedimento è la necessità di informazione al cittadino che transita nelle aree videosorvegliate: gli interessati devono essere informati con cartelli della presenza delle telecamere ed i cartelli devono essere visibili anche quando il sistema è attivo in orario notturno

Il nuovo provvedimento rinvia al modello semplificato di informativa già previsto nel provvedimento del 2004, indicante il titolare del trattamento e la finalità perseguita:

Anche i soggetti pubblici sono tenuti ad osservare le disposizioni in materia di comunicazione e diffusione dei dati ed a fornire l'informativa. Il trattamento può comunque riguardare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali.

Il cartello dovrà rispondere alle seguenti prescrizioni:

• deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;

• deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;

• può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Nel caso in cui l'attività di videosorveglianza sia svolta da forze di polizia o da organi di pubblica sicurezza o altri soggetti pubblici per la tutela dell'ordine o della sicurezza pubblica, nonché alla prevenzione, accertamento o repressione dei reati, l'informativa può essere omessa .

Il Garante, al fine di rafforzare la tutela dei diritti e delle libertà fondamentali degli interessati, ritiene però fortemente auspicabile che l'informativa, benché non obbligatoria, laddove l'attività di

videosorveglianza sia comunque resa in tutti i casi nei quali non ostano in concreto specifiche ragioni di tutela e sicurezza pubblica o di prevenzione, accertamento o repressione dei reati.

Ciò naturalmente all'esito di un prudente apprezzamento volto a verificare che l'informativa non ostacoli, ma anzi rafforzi, in concreto l'espletamento delle specifiche funzioni perseguite, tenuto anche conto che rendere palese l'utilizzo dei sistemi di videosorveglianza può, in molti casi, svolgere una efficace funzione di deterrenza.

Va infine sottolineato che deve essere obbligatoriamente fornita un'idonea informativa in tutti i casi in cui, invece, i trattamenti di dati personali effettuati tramite l'utilizzo di sistemi di videosorveglianza dalle forze di polizia, dagli organi di pubblica sicurezza e da altri soggetti pubblici non siano riconducibili a quelli espressamente previsti dall'art. 53 del Codice (es. utilizzo di sistemi di rilevazioni delle immagini per la contestazione delle violazioni del Codice della strada).

Nel caso di sistemi di videosorveglianza installati da privati collegati con le forze di polizia, tale collegamento deve essere reso noto agli interessati apponendo uno specifico cartello elaborato dal Garante

La violazione delle disposizioni riguardanti l'obbligo di informativa, consistente nella sua omissione o inidoneità è punita con la sanzione amministrativa prevista dall'art. 161 del Codice della Privacy (pagamento di una somma da seimila euro a trentaseimila euro)

5. La verifica preliminare

L' autorizzazione preventiva del Garante per la privacy non è necessaria se vengono attivati sistemi di videosorveglianza nel rispetto dei principi generali dettati nel provvedimento

E' invece richiesta una verifica preliminare attivata d'ufficio o a seguito di un interpello del titolare del trattamento quando vi sono rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare.

In tali ipotesi devono ritenersi ricompresi i sistemi di raccolta delle immagini associate a dati biometrici, per i quali occorre un'autorizzazione preventiva (ad esempio l'incrocio tra immagini ed

impronte digitali per l'accesso negli istituti bancari). E' necessaria l'autorizzazione preventiva del Garante, ad esempio, laddove si preveda una digitalizzazione od indicizzazione delle immagini che consenta una ricerca automatizzata o nominativa, oppure ove vi sia una videosorveglianza dinamico-preventiva, cioè che non riprenda staticamente un luogo ma rilevi percorsi e caratteristiche fisiognomiche delle persone, oppure ancora preveda la ripresa di persone malate o detenute. In linea di massima tali sistemi devono considerarsi eccedenti rispetto alla normale attività di videosorveglianza, in quanto possono determinare effetti particolarmente invasivi della sfera privata ed il loro utilizzo risulta comunque giustificato solo in casi particolari, da verificare sul piano della conformità ai principi di necessità, proporzionalità, finalità e correttezza.

Quindi i cosiddetti **sistemi intelligenti**, quei sistemi di videosorveglianza dotati di software che permettono l'associazione di immagini a dati biometrici (es. "riconoscimento facciale") o in grado, ad esempio, di riprendere e registrare automaticamente comportamenti o eventi anomali e segnalarli (es. "motion detection") è obbligatoria la verifica preliminare del Garante.

Ulteriori casi in cui si rende necessario richiedere una verifica preliminare riguardano l'allungamento dei tempi di conservazione dei dati delle immagini registrate oltre il previsto termine massimo di sette giorni derivante da speciali esigenze di ulteriore conservazione, a meno che non derivi da una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria in relazione a un'attività investigativa in corso

La verifica preliminare è in ogni caso richiesta in tutti i casi in cui i trattamenti effettuati tramite videosorveglianza abbiano natura e caratteristiche tali per cui le misure e gli accorgimenti individuati nel provvedimento del Garante non sono integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare

Il titolare del trattamento di dati personali effettuato tramite sistemi di videosorveglianza non deve richiedere una verifica preliminare purché siano rispettate tutte le seguenti condizioni:

a) il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti;

b) la fattispecie concreta, le finalità del trattamento, la tipologia e le modalità d'impiego del sistema che si intende adottare, nonché le categorie dei titolari, corrispondano a quelle del trattamento approvato;

c) si rispettino integralmente le misure e gli accorgimenti conosciuti o concretamente conoscibili prescritti nel provvedimento adottato dal Garante.

Non si applica il principio del silenzio-assenso: nessuna approvazione implicita può desumersi dal semplice inoltro al Garante di documenti relativi a progetti di videosorveglianza cui non segua un esplicito riscontro dell'Autorità

Ai fini della sicurezza urbana non è invece necessaria **la notificazione**, richiesta solo per il trattamento dei dati previsti dall'art. 37 del Codice della privacy (si tratta di dati sensibili). Non vanno notificati i trattamenti di dati effettuati per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio ancorché relativi a comportamenti illeciti o fraudolenti, quando immagini o suoni raccolti siano conservati temporaneamente.

6. Misure di sicurezza da applicare ai dati personali trattati mediante sistemi di videosorveglianza

Sono tutti gli accorgimenti tecnici ed organizzativi, dispositivi elettronici o programmi informatici utilizzati per garantire che i dati non vadano distrutti o persi anche in modo accidentale, che solo le

persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti.

Nel Codice sono fissati una serie di misure, criteri e procedure (*ad es.*, codice identificativo, *password* per l'accesso ai dati, programmi antivirus, istruzioni per il salvataggio periodico dei dati) che i **titolari** devono adottare

Per i **dati sensibili e giudiziari** sono previste ulteriori misure che si aggiungono alle precedenti, come il ***documento programmatico per la sicurezza* (*dps*),** da redigere ogni anno, e le misure a protezione dei dati da accessi abusivi anche attraverso sistemi di *firewall*.

I dati raccolti mediante sistemi di videosorveglianza devono quindi essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini

Devono essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa

Requisiti minimi:

a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;

b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;

c) per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto

d) nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;

e) qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-*ter* del codice penale;

f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie *wi-fi, wi-max, Gprs*).

7. Responsabili e incaricati

Il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini. Deve trattarsi di un numero delimitato di soggetti, specie quando il titolare si avvale di

collaboratori esterni. Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.)

Il mancato rispetto di quanto previsto comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice. (*sanzione amministrativa da trentamila euro a centottantamila euro)*

L'omessa adozione delle misure minime di sicurezza comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*bis*, (*da diecimila euro a centoventimila euro*) ed integra la fattispecie di reato prevista dall'art. 169 del Codice.[1]

[1] ***Art. 169. Misure di sicurezza***

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni.

All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

CAPITOLO II- SETTORI SPECIFICI

1. La Sicurezza urbana

I Comuni che installano telecamere per fini di sicurezza urbana hanno l'obbligo di mettere cartelli che ne segnalino la presenza, salvo che le attività di videosorveglianza siano riconducibili a quelle di tutela specifica della sicurezza pubblica, prevenzione, accertamento o repressione dei reati.

Per fini di sicurezza urbana la conservazione dei dati è ammessa fino a **7 giorni** che non possono essere superati, fatte salve speciali esigenze.

In ogni caso il Garante ribadisce l'auspicio che, nelle predette ipotesi**, l'informativa, benché non obbligatoria, venga comunque resa,** specie laddove i comuni ritengano opportuno rendere noto alla cittadinanza l'adozione di misure e accorgimenti, quali l'installazione di sistemi di videosorveglianza, volti al controllo del territorio e alla protezione degli individui.

I Comuni e, in generale, i soggetti pubblici operanti sul territorio possono svolgere attività di **videosorveglianza in forma integrata,** tramite la compartecipazione ad un medesimo sistema di rilevazione, al fine di economizzare risorse e mezzi impiegati nell'espletamento delle più diverse attività istituzionali. I sistemi collegano telecamere tra soggetti diversi, sia pubblici che privati, o consentono la fornitura di servizi di videosorveglianza "in remoto" da parte di società specializzate (es. società di vigilanza, Internet providers) mediante collegamento telematico ad un unico centro. In tal caso sono obbligatorie specifiche misure di sicurezza (es. contro accessi abusivi alle immagini) e per alcuni sistemi è comunque necessaria la verifica preliminare del Garante.

In particolare:

a) l'utilizzo condiviso di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando l''accesso a dati che esulano dalle competenze attribuite a ogni singolo ente;

b) nei casi in cui un "centro" unico gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici, i dati personali raccolti dovranno essere trattati in forma differenziata e rigorosamente distinta, in relazione alle competenze istituzionali della singola pubblica amministrazione.

Qualora la natura e le caratteristiche del sistema integrato siano tali da non consentire l'applicazione integrale di tali misure in ragione della natura dei dati o delle modalità del trattamento, è richiesta la verifica preliminare del Garante (es. sistemi di raccolta delle immagini associate a dati biometrici o c.d. intelligenti, cioè in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli ed eventualmente registrarli).

In ogni caso qualora gli Enti locali intendano utilizzare sistemi "intelligenti" di videosorveglianza, basati ad esempio su software di riconoscimento facciale o su tecniche biometriche, gli stessi enti dovranno sottoporre al garante i sistemi per la verifica preliminare.

Il Garante prescive poi l'obbligo di adottare specifiche cautele tecniche in caso di videosorveglianza tramite Internet o utilizzando tecnologie senza fili (WiFi, WiMAX, GPRS), che si sostanziano nell'obbligo di adozione di strumenti di identificazione e di protezione dei sistemi dalle intrusioni esterne e, soprattutto dall'obbligo di utilizzare protocolli di cifratura nella trasmissione delle immagini a distanza.

Il Ministero dell'Interno- Dipartimento della Pubblica Sicurezza- con propria Circolare prot. n. 558/A/421.2/70/195960 del 6 agosto 2010 ha sottolineato che " *"appare importante rilevare come l'utilizzazione di sistemi di videosorveglianza per i luoghi pubblici o aperti al pubblico, qualora si profilino aspetti di tutela dell'ordine e della sicurezza pubblica, oltre a quelli di sicurezza urbana, possa determinare (..) l'affievolimento di alcuni principi di garanzia, quali, in particolare, quello dell'informativa". Sulla questione è però opportuna una valutazione preventiva del comitato provinciale per l'ordine e la sicurezza pubblica. E questa linea interpretativa risulta condivisa anche dall'Anci.*

In sintesi il Ministero richiamando la propria circolare del 8 febbraio 2005 avente ad oggetto la definizione di linee guida in materia di videosorveglianza, quale mezzo di prevenzione e repressione del crimine ribadisce che, pur non essendo necessaria l'informativa per gli impianti comunali di videosorveglianza utilizzati anche per il controllo della sicurezza urbana e dell'ordine pubblico, è ad ogni modo opportuno che sia il comitato provinciale per l'ordine e la sicurezza ad esprimersi preventivamente.

2. Il deposito dei rifiuti

In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi.

Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (art. 13, l. 24 novembre 1981, n. 689).

Il più esteso concetto di sicurezza urbana contenuto nella definizione fornita dal D.L. n. 92/2008, convertito, con modificazioni, in legge 24 luglio 2008, n. 125, per incolumità pubblica si intende l'integrità fisica della popolazione e per sicurezza urbana un bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale".

Pertanto, è da ritenersi consentito, soprattutto ove motivato dall'impossibilità di ricorrere a sistemi diretti, il ricorso alla **videosorveglianza** per l'illecito conferimento dei rifiuti.

I comuni potranno da ora utilizzare sistemi di videosorveglianza per verificare che non vi siano infrazioni amministrative attinenti orari, modalità e svolgimento del deposito dei rifiuti, contrariamente a quanto previsto in precedenza, laddove la videosorveglianza del deposito dei rifiuti era ammessa solo per il controllo di aree abusivamente impiegate come discariche di materiali e di sostanze pericolose.

3. Utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada

Gli impianti elettronici di rilevamento automatizzato delle violazioni, analogamente all'utilizzo di sistemi di videosorveglianza, costituiscono un trattamento di dati personali.

L'utilizzo di tali sistemi è quindi lecito se sono raccolti solo dati pertinenti e non eccedenti per il perseguimento delle finalità istituzionali del titolare, cioè la sicurezza stradale, delimitando a tal

fine l'angolo visuale delle riprese in modo da non raccogliere immagini non pertinenti o inutilmente dettagliate. Il Garante a tal fine prescrive:

a) gli impianti elettronici di rilevamento devono circoscrivere la conservazione dei dati alfanumerici contenuti nelle targhe automobilistiche ai soli casi in cui risultino accertate violazioni in materia di codice della strada. In pratica devono registrare solo i dati indispensabili per la predisposizione del verbale, escludendo la possibilità di registrare dati di terzi estranei.

b) le risultanze fotografiche o le riprese video possono individuare unicamente gli elementi previsti per la redazione del verbale di accertamento delle violazioni (*il tipo di veicolo, il giorno, l'ora e il luogo nei quali la violazione è avvenuta*); deve essere effettuata una ripresa del veicolo che non comprenda o, in via subordinata, mascheri, per quanto possibile, la porzione delle risultanze video/fotografiche riguardanti soggetti non coinvolti nell'accertamento amministrativo (es., pedoni, altri utenti della strada);

c) le risultanze fotografiche o le riprese video rilevate devono essere utilizzate solo per accertare le violazioni delle disposizioni in materia di circolazione stradale e non devono essere inviate d'ufficio al domicilio dell'intestatario del veicolo unitamente al verbale di contestazione, ferma restando la loro accessibilità da parte degli aventi diritto. La documentazione video-fotografica deve essere resa disponibile a richiesta del destinatario del verbale, ma al momento dell'accesso dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo

d) le immagini devono essere conservate per il periodo di tempo strettamente necessario in riferimento alla contestazione, all'eventuale applicazione di una sanzione e alla definizione del possibile contenzioso, fatte salve eventuali esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria;

Anche i conducenti dei veicoli e le persone che accedono o transitano in aree dove sono attivi sistemi elettronici di rilevazione automatizzata delle violazioni devono essere informati in ordine al trattamento dei dati personali. Quindi anche per le postazioni di "**videosorveglianza**" preposte ad accertare violazioni al codice della strada deve essere data informazione della presenza di questi apparecchi mediante l'affissione dell'informativa in maniera ben visibile, dove è indicato che si accede ad una zona video sorvegliata, si specifica il titolare del trattamento e la finalità perseguita dal trattamento dei dati.

Il Garante tuttavia precisa che ove l'informazione della presenza di questi strumenti di "**rilevamento** è già obbligatoria per legge, come nel caso degli apparecchi per la rilevazione della velocità, ai sensi dell'articolo 142, comma 6-bis del codice della strada, non è più necessario utilizzare l'informativa minima, da impiegare unicamente quando la norma speciale nulla dispone. E' stato quindi espressamente ammesso che questa segnaletica può essere considerata idonea "*ad adempiere all'obbligo di fornire l'informativa"*

Quindi qualora già la normativa di settore preveda l'obbligo di rendere nota agli utenti l'installazione degli impianti elettronici di rilevamento automatizzato delle infrazioni (es., rilevamento a distanza dei limiti di velocità, dei sorpassi vietati), l'installazione di tale segnaletica di preavviso assolve già all'obbligo di informativa e permette agli interessati di percepire vari elementi essenziali in ordine al trattamento dei propri dati personali. Pertanto, gli avvisi che segnalano adeguatamente l'attivazione di dispositivi elettronici di rilevazione automatica delle infrazioni possono essere considerati idonei ad adempiere all'obbligo di fornire l'informativa di cui all'art. 13 del Codice della Privacy

Sicuramente, l'informativa minima andrà fornita in tutti gli altri casi in cui sono utilizzati strumenti per accertamento di violazioni diverse, come varchi elettronici per ZTL, centri storici e corsie riservate ovvero quelli che accertano le violazioni semaforiche.

In tali casi, è tuttavia ammesso l'utilizzo anche di avvisi diversi, ancorché non previsti espressamente come obbligatori dalla normativa vigente, ma analoghi a quelli del codice della strada. Le altre forme quale le comunicazioni al pubblico, le iniziative periodiche di diffusa informazione, integrate anche da altre soluzioni quali il volantinaggio, gli annunci televisivi o radiofonici, etc. sono ritenute invece del tutto inappropriate,.

In ogni caso vale la pena di sottolineare come sia consigliabile, anche ad integrazione della segnaletica obbligatoria di presegnalamento delle postazioni fisse o temporanee per l'accertamento delle violazioni, apporre comunque anche il cartello di informativa minima, in modo da evitare qualsiasi pretestuoso tentativo di delegittimare l'operato dell' organo accertatore .

Infine, l'obbligo di fornire tale informativa deve ritenersi soddisfatto anche quando il titolare del trattamento, pur mancando una previsione normativa che obblighi specificamente a segnalare la rilevazione automatizzata, la segnali comunque utilizzando avvisi analoghi a quelli previsti dal Codice della strada.

Qualora si introducano sistemi di rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato, i comuni dovranno rispettare quanto previsto dal D.P.R. 22 giugno 1999, n. 250. Tale normativa prevede che i dati trattati possono essere conservati solo per il periodo necessario per contestare le infrazioni e definire il relativo contenzioso, ferma restando l'accessibilità agli stessi per fini di polizia giudiziaria o di indagine penale

4. Attivita' specifiche

a) Rapporti di lavoro

Nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa. Pertanto è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul *badge*). Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell'art. 4 della l. n. 300/1970 (Statuto Lavoratori), gli impianti e le apparecchiature, "*dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti"*

Tali garanzie vanno osservate sia all'interno degli edifici, sia in altri contesti in cui è resa la prestazione di lavoro, come, ad esempio, nei cantieri edili o con riferimento alle telecamere installate su veicoli adibiti al servizio di linea per il trasporto di persone o su veicoli addetti al servizio di noleggio con conducente e servizio di piazza (taxi) per trasporto di persone (le quali non devono riprendere in modo stabile la postazione di guida) e le cui immagini, raccolte per finalità di sicurezza e di eventuale accertamento di illeciti, non possono essere utilizzate per controlli, anche indiretti, sull'attività lavorativa degli addetti.

L'utilizzo di sistemi di videosorveglianza preordinati al controllo a distanza dei lavoratori o ad effettuare indagini sulle loro opinioni integra la fattispecie di reato prevista dall'art. 171 del Codice.

Eventuali riprese televisive sui luoghi di lavoro per documentare attività od operazioni solo per scopi divulgativi o di comunicazione istituzionale o aziendale, e che vedano coinvolto il personale dipendente, possono essere assimilati ai trattamenti temporanei finalizzati alla pubblicazione

occasionale di articoli, saggi ed altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull'attività giornalistica

b) Ospedali e luoghi di cura

L'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (ad es. unità di rianimazione, reparti di isolamento), stante la natura sensibile di molti dati che possono essere in tal modo raccolti, devono essere limitati ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute degli interessati.

Devono essere inoltre adottati tutti gli ulteriori accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate,

Le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse. In tale quadro, va assolutamente evitato il rischio di diffusione delle immagini di persone malate su *monitor* collocati in locali liberamente accessibili al pubblico.

c. . Istituti scolastici

L'eventuale installazione di sistemi di videosorveglianza presso istituti scolastici deve garantire *"il diritto dello studente alla riservatezza"*, prevedendo opportune cautele al fine di assicurare l'armonico sviluppo delle personalità dei minori in relazione alla loro vita, al loro processo di maturazione ed al loro diritto all'educazione

Il Garante ritiene ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate, attivando però gli impianti negli orari di chiusura degli istituti; è vietato, attivare le telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche che si svolgono all'interno della scuola.

Laddove la ripresa delle immagini riguardi le aree perimetrali esterne degli edifici scolastici, l'angolo visuale deve essere delimitato alle sole parti interessate,

d. Sicurezza nel trasporto pubblico

Alcune situazioni di particolare rischio possono fare ritenere lecita l'installazione di sistemi di videosorveglianza sia su mezzi di trasporto pubblici, sia presso le fermate dei predetti mezzi.. Occorre però evitare riprese particolareggiate nei casi in cui le stesse non sono indispensabili in relazione alle finalità perseguite.

In ogni caso i titolari del trattamento dovranno provvedere a fornire la prevista informativa agli utenti del servizio di trasporto urbano. Gli autobus, i tram, i taxi ed i veicoli da noleggio con o senza conducente dotati di telecamere dovranno pertanto portare le apposite indicazioni che diano conto della presenza dell'impianto di videosorveglianza,

Presso le aree di fermata, in prossimità delle quali possono transitare anche soggetti diversi dagli utenti del servizio di trasporto pubblico, l'angolo visuale delle apparecchiature di ripresa deve essere strettamente circoscritto all'area di permanenza, permettendo l'inquadratura solo della pensilina e di altri arredi urbani funzionali al servizio di trasporto pubblico (tabelle degli orari, paline recanti l'indicazione degli autobus in transito, ecc.), con esclusione della zona non immediatamente circostante e comunque dell'area non direttamente funzionale rispetto alle esigenze di sicurezza del sistema di traffico e trasporto. Anche in tale ipotesi occorre evitare le riprese inutilmente particolareggiate o tali da rilevare caratteristiche eccessivamente dettagliate degli individui che stazionano presso le fermate. Dell'esistenza delle telecamere deve essere fornita adeguata informativa

e.. Utilizzo di web cam o camera-on-line a scopi promozionali-turistici o pubblicitari
Le attività di rilevazione di immagini a fini promozionali-turistici o pubblicitari, attraverso *web cam* devono avvenire con modalità che rendano non identificabili i soggetti ripresi: le immagini raccolte

tramite tali sistemi, infatti, vengono inserite direttamente sulla rete Internet, consentendo a chiunque navighi sul web di visualizzare in tempo reale i soggetti ripresi e di utilizzare le medesime immagini anche per scopi diversi dalle predette finalità promozionali-turistiche o pubblicitarie perseguite dal titolare del trattamento.

CAPITOLO III - GLI ADEMPIMENTI DEI COMUNI CHE INTENDONO INSTALLARE UN IMPIANTO DI VIDEOSORVEGLIANZA

1. Trattamento dati personali, titolare, responsabile, incaricato del trattamento dati.

1.1 Il trattamento

è un'operazione o un complesso di operazioni che hanno per oggetto, operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

È "**dato personale"**, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale, mentre sono dati identificativi i dati personali che permettono l'identificazione diretta dell'interessato. Quindi è "dato personale" il suono, oppure l'immagine proveniente da un sistema di videosorveglianza, anche se queste informazioni non vengono immagazzinate in un archivio elettronico e comunicate a terzi ed anche dove le persone non possano essere identificate direttamente ma soltanto tramite il collegamento con altre fonti conoscitive, quali foto segnaletiche, data-base, archivi di polizia, identikit e quant'altro.

Si definiscono **"dati sensibili",** invece, quelli idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

Esiste un'altra particolare categoria di dati, equiparata ai "dati sensibili". Sono "**dati giudiziari**", quelli idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale

Per garantire il corretto trattamento dei dati personali, il Codice ha previsto una piramide di responsabilità in capo a diversi soggetti:

a) Il titolare del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza; quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, attraverso il suo legale rappresentante **(Sindaco),** ivi compreso i profili della sicurezza**.**

b) Il responsabile del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali **(Il Comandante o ufficiale delegato)** Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare, per cui il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare

il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni e delle proprie istruzioni.

c) **Gli incaricati del trattamento dei dati**, sono le persone fisiche **(i singoli operatori)** autorizzate dal titolare o dal responsabile a compiere operazioni di trattamento. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. Anche in questo caso la designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito.

1.2 La conservazione dei dati

Il garante considera eventuale la conservazione temporanea dei dati, nel rispetto dei principi di necessità e proporzionalità, ma deve essere commisurata al tempo necessario - e predeterminato - a raggiungere la finalità perseguita.

La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati (non comunque superiore alla settimana).

Per i comuni e **nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana,** il termine massimo di durata della conservazione dei dati è esteso *"ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione"*.

In tutti i casi in cui si voglia procedere per motivi comunque eccezionali e sempre nel rispetto del principio di proporzionalità, ad un allungamento dei tempi di conservazione per un periodo superiore alla settimana, occorre procedere ad una verifica preliminare del Garante. La congruità di un termine di tempo più ampio di conservazione va adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità. La relativa congruità può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso.

Il software deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

1.3 La sicurezza nella conservazione dei dati raccolti mediante la videosorveglianza

I dati raccolti devono essere protetti, soprattutto dagli accessi non autorizzati, adottando tutte quelle soluzioni possibili con la migliore tecnologia e le opportune scelte organizzative, in modo che sia precluso il trattamento a terzi non autorizzati e che sia sempre tracciabile ogni accesso effettuato. Devono essere evitati gli accessi non necessari durante le operazioni di manutenzione delle apparecchiature, che dovranno avvenire sempre in presenza di soggetti accreditati all'accesso. Per quanto riguarda i sistemi informatici, essi devono essere protetti dagli accessi abusivi e, se è prevista la trasmissione dei dati tramite tecnologie WI-FI o simili, questa deve essere protetta tramite crittografia del segnale.

L'accesso sarà consentito unicamente per le finalità già stabilite per il trattamento dei dati, differenziando le competenze e quindi i livelli di accesso, mediante il rilascio di specifiche credenziali di autenticazione.

Inoltre, onde evitare l'indebita conservazione delle immagini, devono essere predisposte adeguate soluzioni tecniche od organizzative, idonee alla cancellazione delle registrazioni quando sia venuta meno la necessità di mantenerle nell'archivio.

Ovviamente, questi sistemi di protezione, al di là di quelli che possono essere adottati con la migliore organizzazione degli accessi, devono essere commissionati ai tecnici dell'amministrazione, ovvero a tecnici esterni, con apposito incarico.

2. il regolamento

Vedasi allegato B

3. Il documento di liceità (*già piano di documentazione delle scelte*)

Le ragioni delle scelte, relative al trattamento dei dati personali mediante videosorveglianza, "devono essere adeguatamente documentate in un atto autonomo conservato presso il titolare e il responsabile del trattamento e ciò anche ai fini dell'eventuale esibizione in occasione di visite ispettive, oppure dell'esercizio dei diritti dell'interessato o di contenzioso".

Esso deve indicare quali soluzioni operative del sistema di videosorveglianza sono state adottate, i motivi di tali scelte le finalità perseguite

Il documento delle scelte deve quindi indicare:

1)se sia sufficiente, ai fini della sicurezza, rilevare immagini che non rendono identificabili i singoli cittadini, anche tramite ingrandimenti, ovvero se sia realmente essenziale, ai fini prefissi, raccogliere immagini dettagliate e per quale motivo;

2)quali dati vengono rilevati e se essi vengono o meno registrati e, in tale caso, per quale periodo di tempo verrà conservata la registrazione e il motivo di tale scelta, indicando eventualmente i casi precedenti a cui si fa riferimento per giustificare tale scelta;

3) se ci si avvale di una rete di comunicazione o una banca di dati indicizzata, ovvero se si utilizzano funzioni di fermo-immagine o tecnologie digitali, anche se abbinate ad altre informazioni o interconnesse con altri sistemi gestiti dallo stesso titolare o da terzi, ed il motivo di tale scelta;

4) se avviene la ripresa di luoghi privati o accessi di edifici e per quale motivo;;

5) i soggetti designati quali incaricati del trattamento dei dati (a visionare le immagini), anche se soggetti "esterni" al titolare, e la diversificazione dei diversi livelli di accesso al sistema e all'utilizzo delle informazioni con esso raccolte, anche con riferimento alle eventuali esigenze di manutenzione.

4. Documento programmatico sulla sicurezza

Il "Documento Programmatico sulla Sicurezza" (di seguito DPS), predisposto ai sensi dell'art. 34 del Decreto Legislativo 196/03 nei modi previsti dal punto 19 dell'Allegato B dello stesso, **deve essere redatto qualora vengano trattati dati sensibili o giudiziari con strumenti elettronici**. Tale documento deve essere tenuto sempre aggiornato.

La sua finalità è sia proteggere il patrimonio informativo degli Enti da attività (ivi inclusa la videosorveglianza) che possono comportare il maltrattamento dei dati personali, sia limitare gli effetti causati dall'eventuale occorrenza di tali cause.

Il **DPS** deve contenere idonee informazioni riguardo:

a) l'elenco dei trattamenti di dati personali;

b) la distribuzione dei compiti e delle responsabilità;

c) l'analisi dei rischi che incombono sui dati;

d) le misure da adottare per garantire la riservatezza

e) la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati;

f) la previsione di interventi formativi degli incaricati del trattamento;

g) la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare;

h) l'individuazione dei criteri da adottare per la cifratura o per la separazione dei dati personali idonei a rilevare lo stato di salute e la vita sessuale dagli altri dati personali dell'interessato (per organismi sanitari e gli esercenti le professioni sanitarie).

i) l'integrità e la disponibilità dei dati,

l) la protezione delle aree e dei locali;

Il Garante pone a disposizione degli operatori sul proprio sito una **Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS)** , utilizzabile facoltativamente, per redigere ed aggiornare il documento programmatico sulla sicurezza, soprattutto nelle realtà piccole e medie dimensioni,

CAPITOLO IV - LE PRONUNCE DEL GARANTE

Il vicepresidente dell'Autorità garante per la protezione dei dati personali **Giuseppe Chiaravalloti,**, ha fornito alcune spiegazioni e suggerimenti pratici in relazione al nuovo provvedimento dell'8 aprile 2010

Che fare:

a) Nel recente provvedimento in materia di videosorveglianza non si rinviene più «l'atto di documentazione delle scelte».
La mancata previsione deve essere inquadrata nell'ottica di semplificazione che questa Autorità già sta perseguendo da tempo e che consente ai titolari del trattamento di rispettare la normativa seguendo poche ma chiare, inderogabili e incisive regole per la protezione dei dati personali degli individui. Un atto del medesimo contenuto che evidenzi le motivazioni dei provvedimenti è tuttavia necessario a sostegno degli atti deliberativi e le determinazioni dell'ente locale o delle richieste di verifica preliminare al garante.

b) I sistemi di lettura targhe abbinate a banca dati dei proprietari dei veicoli non rientrano tra gli esempi citati nel provvedimento né per quanto riguarda l'obbligo di verifica preliminare, né per quanto concerne la sicura esclusione da tale obbligo.
Non è necessaria la verifica preliminare dal garante se i sistemi di videosorveglianza si limitano a una lettura delle targhe, senza altre associazioni con altri dati tali da provocare pregiudizio per gli interessati, non deve essere adempiuto l'obbligo previsto dall'art. 17 del Codice. L'obbligo di verifica preliminare deve essere adempiuto quando l'associazione delle immagini avvenga con altri particolari dati (quali sono i dati biometrici o dati sensibili) e non con qualsiasi tipologia di dato personale

c) Videosorveglianza con telecamere mobili (per esempio sulle vetture delle polizie locali) e obbligo di informativa
È sufficiente un'indicazione segnaletica sul veicolo su cui è posizionata la telecamera mobile, collocata in modo tale da essere immediatamente visibile anche a una certa distanza.
La ratio sottostante all'obbligo di informativa è quella di consentire a ogni interessato di avere la possibilità di sapere che si stanno effettuando delle riprese e, eventualmente, di adeguare il suo comportamento in relazione a tale consapevolezza.

Plurime finalità per l'ente locale (sicurezza urbana e diverse): necessaria l'informativa e necessaria la verifica preliminare dal garante, soprattutto per stabilire il periodo massimo di conservazione
Se una delle finalità perseguite dal titolare del trattamento richiede l'obbligo di rendere previa informativa, essa deve essere fornita anche laddove non sia necessaria per tutte le altre finalità.
Se una delle finalità perseguite consente un termine di conservazione fino a sette giorni (come nel caso di esigenze di sicurezza urbana), ma le immagini sono trattate anche per altre finalità il cui termine massimo di conservazione dei dati è minore, il titolare del trattamento deve sottoporre la questione all'Autorità attraverso lo strumento della verifica preliminare.
Il caso è quello dei sistemi di videosorveglianza per la sicurezza urbana che vengono usati anche per altre finalità di diversa natura, per esempio il controllo sull'abbandono di rifiuti. La finalità di sicurezza urbana esonera dall'obbligo di informativa e prevede un periodo più lungo di conservazione delle immagini (una settimana). In caso di videosorveglianza promiscua bisogna richiedere la verifica preliminare al Garante

Verifica preliminare dal garante per videosorveglianza intelligente
Bisogna sempre passare dal garante per la videosorveglianza «intelligente» e cioè quella che si attiva a fronte di condotte anomale, e ciò anche se si tratta di motion detection basilare (e cioè senza sofisticato tracciamento del percorso delle persone).

Una panoramica su alcune precisazioni del Garante

LUOGHI DI CULTO

Nel proprio provvedimento del 2004 il Garante raccomandava particolari cautele nell'installazione di sistemi di videosorveglianza presso chiese o altri luoghi di culto o di ritrovo di fedeli in funzione dei rischi di un utilizzo discriminatorio delle immagini raccolte e del carattere sensibile delle informazioni relative all'appartenenza ad una determinata confessione religiosa.

Al fine di garantire il rispetto dei luoghi di sepoltura per la sussistenza di dati particolarmente sensibili, l'installazione di sistemi di videosorveglianza deve ritenersi ammissibile all'interno di tali aree solo quando si intenda tutelarle dal concreto rischio di atti vandalici

SEMAFORI SPIA" E MULTE DA PAGARE

A proposito della legittimità dei "semafori spia" Si tratta, infatti, di apparecchi in termini generali leciti, per i quali, peraltro, nell'ipotesi in cui siano destinati a rilevare gli accessi ai centri storici, è stato emanato un apposito regolamento che ha seguito le indicazioni del Garante (D.P.R. 250/1999).

Non è prevista per l'installazione di questo tipo di "semplici" telecamere, il rilascio di una formale autorizzazione preventiva, generale o caso per caso, da parte del Garante. Di conseguenza, i verbali di contestazione non devono menzionare tale specifica autorizzazione.(newsletter 11.7.2004)

TRASMISSIONE DELLE SEDUTE PUBBLICHE DEL CONSIGLIO COMUNALE VIA INTERNET, MA NIENTE WEBCAM PER LE RIUNIONI DI GIUNTA E PER GLI INCONTRI DEL SINDACO CON I CITTADINI.

Garante ha precisato che la diffusione via Internet di alcune iniziative caratterizzate di per se stesse da un obiettivo di ampia conoscenza nel pubblico, come conferenze stampa, riunioni di consiglio ecc., non pone particolari problemi dal punto di vista della legge sulla privacy.

E' necessario però informare tutti i presenti della diffusione delle immagini, anche attraverso affissione di avvisi chiari e sintetici ed osservare poi una particolare cautela per i dati sensibili, per i quali va rigorosamente rispettato il principio di stretta necessità, evitando in ogni caso di diffondere dati idonei a rivelare lo stato di salute di singoli cittadini.

Le webcam che riproducono anche il sonoro non sono, invece, utilizzabili per le riunioni di organi che, in base a leggi o regolamenti, non sono aperte al pubblico, quali ad esempio le riunioni della giunta comunale o di varie commissioni.

Stesso discorso vale per il ricevimento del pubblico e l'ordinaria attività degli uffici. Le comprensibili finalità di comunicazione con i cittadini e di trasparenza non possono, ha spiegato il Garante, essere perseguite imponendo a ciascun cittadino un obbligo di diffondere la propria immagine durante i colloqui con il sindaco o con un altro rappresentante comunale, o, addirittura, di rivelare al pubblico il contenuto della conversazione, che potrebbe riguardare delicati aspetti personali o familiari.

Il dialogo dei rappresentanti eletti con i cittadini non può, infatti, secondo il Garante, esporre ogni persona che chieda un incontro ad una pubblicità indiscriminata.

Inoltre, ha ricordato l'Autorità, la riproduzione stabile di immagini applicata all'ordinaria attività degli uffici può comportare anche un controllo a distanza della qualità o della quantità del lavoro dei dipendenti comunali, vietato in base allo Statuto dei lavoratori.(newsletter 26.5.2001)

TELECAMERE CON "VISTA"

Garantire la sicurezza di un quartiere non giustifica la presenza di telecamere che, anche in modo occasionale e involontario, riprendano interni di abitazioni private, violando in questo modo la privacy dei cittadini che vi risiedono. É quanto stabilito dal Garante nell'operare sulla segnalazione di un cittadino, che riteneva leso il proprio diritto alla riservatezza dalla presenza di diverse telecamere installate dal comune in prossimità del proprio stabile e in grado di "guardare" fin all'interno delle abitazioni.

Le telecamere, come dichiarato dal comune, erano state posizionate, oltre che per monitorare il traffico, anche per esigenze di maggiore sicurezza dei cittadini, tutela del patrimonio e controllo di determinate aree.

In un primo momento il comune aveva comunicato che l'impianto era programmato in modo da non riprendere edifici privati ed era comunque in grado, attraverso un sistema di mascheratura dinamica delle finestre, eventualmente riprese, di garantire la riservatezza delle persone. Tuttavia dopo aver visionato alcune foto presentate dal ricorrente, l'Autorità ha disposto un sopralluogo dal quale è emerso che il tipo di telecamera installata ("Dome") permette facilmente zoom, brandeggio e identificazione dei tratti somatici delle persone che vengono riprese. Pur non essendo posizionate in direzione delle abitazioni, il sistema consente a qualsiasi operatore, che abbia accesso diretto al server, di spostare le telecamere nelle diverse angolazioni e operare così un'intromissione ingiustificata nella vita privata degli interessati.

Valutati questi elementi il Garante ha stabilito che, per utilizzare lecitamente il sistema di videosorveglianza, il comune deve adottare ogni accorgimento volto ad evitare la ripresa di persone in abitazioni private; dovrà delimitare, quindi, la dislocazione, l'uso dello zoom e, in particolare, l'angolo visuale delle telecamere in modo da escludere ogni forma di ripresa, anche quando non c'è registrazione, di spazi interni di abitazioni private, attraverso eventuali sistemi di settaggio e oscuramento automatico, non modificabili dall'operatore. Il comune dovrà integrare inoltre il modello di informativa indicando, oltre al monitoraggio del traffico, le finalità di sicurezza e di controllo di sua competenza.(newsletter 19.11.2007)

I VIDEOCITOFONI

Per rispondere a quesiti rivolti spesso dai cittadini: I videocitofoni sono ammessi per finalità identificative dei visitatori, che si accingono ad entrare in luoghi privati Tali apparecchiature, che rilevano immagini e suoni senza registrazioni, sono dislocate abitualmente all'ingresso di edifici o immobili in corrispondenza di campanelli o citofoni, appunto per finalità di controllo dei visitatori che si accingono ad entrare. La loro esistenza deve essere conosciuta attraverso una informativa agevolmente rilevabile, quando non sono utilizzati per fini esclusivamente personali

CAP. V - UN PO' DI GIURISPRUDENZA

La Cassazione delimita le zone nelle quali può essere attivata la videosorveglianza rispettando la privacy e conferma la condanna di un cittadino che "spiava" la vicina in quanto la privacy di una persona viene lesa non solo "nei luoghi di privata dimora", ma anche "nelle pertinenze di essi". Con la *sentenza 25666 del 4.4.2003* la Corte ha confermato la condanna di un cittadino per "interferenze illecite nella vita privata", poichè aveva ripreso con una telecamera le attività svolte da una vicina nel garage dove erano custodite le macchine. Per la Suprema Corte queste riprese ledono "il diritto alla riservatezza della vita individuale dalle interferenze illecite altrui". La Corte ha quindi delineato le zone dove può essere attivata la videosorveglianza senza compiere il reato di interferenza illecita nella vita privata (art. 615 bis c.p.): ad esempio chi sorveglia il cittadino in un garage, anche se aperto al pubblico, sul pianerottolo o davanti all'ingresso di casa commette reato
Secondo la Cassazione, il divieto di "sorveglianza" deve essere applicato su tutte le cose che siano legate con l'abitazione o con altro luogo di privata dimora da stretto rapporto pertinenziale **ai sensi dell'art. 817 c.c.,** come ad esempio, gli ingressi, anche se prospicienti sulla pubblica via, "non potendosi confondere il diritto civilistico di veduta con la facoltà (soggetta a restrizioni penalmente garantite) di documentare fatti della vita privata altrui**".**

La sentenza della Corte di Cassazione *(16.9.97 n° 9211*) stabilisce che gli accordi stipulati per installare la videosorveglianza sono illegittimi se sottoscritti tra le Segreterie delle Organizzazioni Sindacali e l'Azienda perché, come chiaramente espresso dall'art. 4 dello Statuto dei Lavoratori, sono le RSA i soggetti individuati per la sottoscrizione degli accordi in materia.
In difetto di tale accordo, sempre l'art. 4 dello Statuto dei Lavoratori autorizza il datore di lavoro a richiedere l'autorizzazione del Servizio Ispezione Lavoro, che potrà dettare le modalità d'uso della videosorveglianza

La Quinta Sezione Civile della Corte di Cassazione *(Sent. n. 44156/2008*) ha stabilito che è lecita la videosorveglianza nei condomini e ciò anche se è a discapito della privacy. Nel caso di specie, la Corte ha infatti osservato che "non era certamente volontà dell'imputato, che secondo le stesse sentenze di merito aveva installato l'impianto solo per ragioni di sicurezza esterne, riprenderne anche aspetti della vita privata dei suoi vicini all'interno della loro casa: e di tanto danno atto indirettamente le stesse decisioni di merito, evidenziando che l'angolazione delle telecamere consentiva la visuale solo incidentale di piccole porzioni di uno sporto e di un poggiolo, non interessandosi affatto del tipo e della estensione di tale visuale e soprattutto ricordando che l'imputato aveva fornito ai vicini la possibilità di controllare quanto visualizzato dalle telecamere mediante i televisori all'interno delle loro case. Sicchè può concludersi che, in relazione alla ripresa di immagini attinenti alla vita privata svolgentesi in ambito domiciliare protetto, difetta comunque l'elemento soggetto del reato.

L'uso di una telecamera a circuito chiuso, finalizzata a controllare a distanza anche l'attività dei dipendenti, è illegittimo e come tale, sul piano processuale, non può avere alcun valore probatorio (sentenza della Cassazione n. *8250/2000*) ad esempio, ai fini della richiesta di risarcimento danni per la sottrazione di merci aziendali.

La stessa conclusione può essere applicata per le sanzioni disciplinari, poiché la Cassazione ha dato una risposta affermativa nella sentenza n. *15892/2007* sostenendo che i dati acquisiti tramite videosorveglianza in violazione dello Statuto dei lavoratori non possono essere un legittimo fondamento per un licenziamento.

Corte di Cassazione, sez. V penale, *18 marzo 2010 n. 20722* ha statuito come sia legittima l'installazione di impianti di videosorveglianza da parte del datore di lavoro, allorquando questi abbia sospetti circa eventuali fatti illeciti commessi dal lavoratore. Le registrazioni risultano, peraltro, utilizzabili anche nel processo penale. Resta precluso al datore di lavoro, a norma dello Statuto dei lavoratori, l'impianto di sistemi di videoregistrazione per un generalizzato controllo a distanza dell'attività dei lavoratori.

CAP. VI - USO DELLA VIDEORIPRESA NEL CORSO DELLE INDAGINI DI POLIZIA GIUDIZIARIA.

La videosorveglianza, per il solo fatto di catturare le immagini di un evento criminale, dovrebbe agevolare le indagini di polizia giudiziaria per identificare i responsabili di reati.

La registrazione delle immagini, quali mezzo di prova a fini processuali penali, non trova una specifica regolamentazione nel vigente Codice di procedura penale. In altre parole, le regole attuali del Codice non inquadrano, a fini giudiziari, tale mezzo di prova, e ciò anche quando le immagini siano state "catturate", direttamente, dalla Polizia giudiziaria.

Stante la carenza normativa, è stata la giurisprudenza a fornire chiarimenti sull'utilizzo processuale delle immagini, interpretando allo scopo le norme generali in tema di prove.

L'attenzione dei giudici si è diretta, innanzitutto, sulle immagini raccolte nell'ambito di luoghi pubblici. A questo proposito, la prevalente giurisprudenza, e in particolare quella di legittimità, ritiene che le immagini concernenti luoghi pubblici o aperti al pubblico siano utilizzabili in sede processuale, sia che derivino da opera investigativa della Polizia giudiziaria, sia che siano ottenute da impianti privati di videsosorveglianza.

Occorre a questo punto ricordare che, secondo la prevalente interpretazione, «*luogo pubblico*» è quello a cui può accedere liberamente qualsiasi persona. Così, ad esempio, una pubblica via o una piazza di uno dei nostri Comuni. Sono invece da considerare *luoghi aperti al pubblico* quelli in cui l'accesso è sostanzialmente aperto, ma soggetto a regole: ad esempio, un luogo con orari di apertura e chiusura.

Secondo la Cassazione (Sezioni Unite, sentenza n. 26795/2006) le immagini "captate" in tali contesti fisici sono, di regola, potenzialmente "sfruttabili" in sede giudiziaria. I giudici distinguono, tuttavia, specificando che:

a) le immagini riprese nel corso di specifica attività investigativa fanno parte di quest'ultima e possono essere introdotte nel processo come "prove atipiche" secondo le regole di cui all'articolo 189([1]) del Codice di procedura penale. In questo caso la normativa vigente non detta un divieto di loro utilizzo processuale, ma chiarisce che spetterà al giudice valutare, in contraddittorio con le parti, se ammettere o meno le immagini ottenute mediante riprese in un luogo pubblico o aperto al pubblico, come mezzo di prova.

b) le videoregistrazioni, realizzate fuori dal procedimento penale, sono da considerare «documento» e in tal senso sottoposte allo specifico regime di cui all'articolo 234([2]) del Codice di procedura penale; occorre però che tali immagini registrate non interferiscano con il luogo di privata dimora altrui, perché in tal caso la prova sarebbe illecita e addirittura lesiva dell'art. 14 della Costituzione che sancisce l'inviolabilità del domicilio. In tal caso si tratterebbe di un'intercettazione ambientale,

---

([1]) *Art. 189 C.P.P.. Prove non disciplinate dalla legge.*
1. Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova.

([2]) *Art. 234 C.P.P.. Prova documentale.*
1. E' consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo.
2. Quando l'originale di un documento del quale occorre far uso è per qualsiasi causa distrutto, smarrito o sottratto e non è possibile recuperarlo, può esserne acquisita copia.
3. E' vietata l'acquisizione di documenti che contengono informazioni sulle voci correnti nel pubblico intorno ai fatti di cui si tratta nel processo o sulla moralità in generale delle parti, dei testimoni, dei consulenti tecnici e dei periti.

consentita soltanto nei casi e con le modalità richieste dalla legge (richiesta da parte del P.M. e l'autorizzazione da parte del G.I.P.)

Se l'autorità di polizia opera con un sistema di videosorveglianza, ad esempio perché in una determinata zona del territorio c'è attività di spaccio di sostanze stupefacenti, è del tutto evidente che ciò esonera l'autorità stessa dal rispetto di quelle che sono le norme a tutela della riservatezza. In tal caso, nel bilanciamento degli interessi, cede la tutela della riservatezza a favore della sicurezza pubblica. A ciò si aggiunge che se gli investigatori videoriprendono un luogo pubblico o aperto al pubblico, tale attività non costituisce intercettazione ambientale e quindi si agisce al di fuori dei limiti imposti dalla disciplina della privacy.

Nel complesso, si può, pertanto sostenere che, nel vigente Codice di procedura penale, le riprese "captate" in un luogo pubblico con telecamere non sono soggette a particolari limiti, perché, come chiarisce la Cassazione (Sezione IV penale, sentenza n. 7063/2000), la natura pubblica del luogo presuppone che chi mette in atto delle condotte in tale ambito fisico rinunzia alla propria riservatezza. Le riprese effettuate dalla polizia giudiziaria in luoghi pubblici o aperti al pubblico non incidono, pertanto, su diritti quali quello all'inviolabilità del domicilio e non richiedono una preventiva autorizzazione dell'autorità giudiziaria. La conseguenza giuridica di tutto ciò è che, allo stato attuale delle norme, esse rappresentano concretamente un importante "strumento" di prova.

A ben diverse conclusioni giuridiche, di conseguenza, si giunge relativamente alle riprese interessanti luoghi privati, in specie dimore private o altri ambiti soggetti ad una certa tutela della "privacy": come nel caso di toilette o di club privè.

Sulla scia delle Sezioni Unite, in altre recenti sentenze la Suprema Corte ha considerato legittime e, di conseguenza, utilizzabili in giudizio le videoregistrazioni effettuate dalla polizia giudiziaria con una telecamera (posizionata all'esterno) che inquadrava e riprendeva l'ingresso, i balconi ed cortile del domicilio dell'indagato, luoghi che sono stati definiti "esposti al pubblico" perché caratterizzati da una libera percettibilità esterna; la tutela di cui all'art.14 Cost. verrebbe dunque meno sol perché l'area interessata dalle riprese ricade nella sfera visiva di un numero indifferenziato di persone

Quand'è che il trattamento dei dati è illecito? Se è prefissa una determinata finalità, operare in difformità di questa può costituire reato. Un esempio: se installo una videocamera davanti alla porta di casa mia -quindi eseguo un'attività lecita- e casualmente un personaggio famoso ha un approccio intimo nello specifico raggio d'azione della telecamera e viene ripreso, bene, non ho commesso alcun reato, perché sarà stato il personaggio famoso ad inserirsi, ancorché involontariamente nella mia sfera; però se questo dato lo prendo e lo cedo ad un settimanale per finalità di lucro è evidente che ciò integra il reato previsto dall'art. 167 della legge 196/2003. Il dato viene acquisito lecitamente ma trattato illecitamente.

Bisogna però sempre tenere presente che quando si parla di inutilizzabilità per illecito trattamento del dato, si fa riferimento alle finalità originariamente prefisse per la videosorveglianza Anche l'immagine acquisita in maniera *illecita* potrebbe essere utilizzata laddove risulti utile nell'ambito di un processo, secondo lo specifico regime di cui all'articolo 234 c.p.p., vale a dire se un'immagine è stata acquisita *illecitamente* perché le finalità della videosorveglianza erano tutt'altre, ma questa risulta utile per provare la colpevolezza di un imputato, o per scagionarlo, è evidente che anche il dato acquisito illecitamente potrà essere utilizzabile.

Le videoregistrazioni operate in luoghi pubblici ovvero aperti od esposti al pubblico, se eseguite dalla polizia giudiziaria nell'ambito del procedimento penale, costituiscono prova atipica che non necessita dell'autorizzazione del G.i.p., e, documentando attività investigative non ripetibili, possono essere allegate al relativo verbale ed inserite nel fascicolo per il dibattimento. (Fattispecie in cui la P.G. aveva installato telecamere sulla pubblica via per verificare il flusso di automezzi e

persone in arrivo ed in partenza dal covo degli imputati (Cass. pen. Sez. II *Sent., 24/04/2007, n. 35300)*

In relazione all'attività di controllo - prevista dall'art. 197, comma 3, D.Lgs. n. 152/2006 - su imprese che svolgono attività di gestione dei rifiuti, sono da ritenersi legittime e pertanto utilizzabili le videoregistrazioni del luogo (nella specie, una discarica di rifiuti) eseguite dalla p.g., non rappresentando esse un'indebita intrusione né nell'altrui privata dimora, né nell'altrui domicilio. L'impiego della video camera è perciò equiparabile ad un'operazione eseguita nei limiti dell'autonomia investigativa (*07/04/2009, n. 28474)*

Sono probatoriamente utilizzabili le videoregistrazioni effettuate dalla persona offesa di reiterati atti vandalici e di danneggiamento ai danni della porta del proprio appartamento, della porta dell'attiguo garage e della cassetta postale antistante l'ingresso dell'appartamento, dal momento che l'area interessata dalle videoregistrazioni, operate con telecamera sita all'interno dell'appartamento, ricade nella fruizione di un numero indifferenziato di persone e non attiene alla sfera di privata dimora di un singolo soggetto. (Cass. pen. Sez. II, *10/11/2006, n. 5591*

Un cenno merita infine la disciplina della **registrazione digitale delle immagini**, quali mezzo di prova a fini processuali penali, che trova una specifica regolamentazione **nella legge n. 48/08**([3]). Gli artt. 8 e 9 della legge hanno modificato e adattato alle realtà informatiche le disposizioni codicistiche in materia di ispezioni, perquisizioni e sequestri, operati dal Pubblico Ministero o, in caso di urgenza dalla Polizia Giudiziaria. Nella nuova formulazione gli artt. 244, 247 c.p.p. (e parimenti agli artt. 352 e 354 c.p.p.) impongono all'Autorità Giudiziaria, in sede di **ispezioni o perquisizioni di sistemi informatici o telematici**, di adottare "*misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*, prescrivendo quindi l'adozione obbligatoria di procedure che garantiscano l'integrità dei dati informatici, salvaguardando il diritto di difesa.

Inoltre, gli artt. 254 *bis*, 256, 260 e 354 c.p.p. prescrivono l'acquisizione dei dati informatici "*mediante copia…su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità*".

Quindi, una volta acquisita l'immagine, occorre verificare come "trattare" l'immagine acquisita ai fini probatori nel processo penale. A tal fine è necessario precisare che il risultato della videosorveglianza è un dato digitale - una sequenza di numeri binari - all'interno della quale è contenuta un'informazione digitale attinente ad un'indagine – la foto di un viso, un filmato di un'auto, ecc. E' di primaria importanza, quindi, la necessità di preservare il dato digitale e di studiare l'informazione digitale. Il legislatore, con le modifiche apportate dalla legge n. 48/08 al Codice di Procedura Penale, impone la cura assoluta nel repertare la prova e nel conservarla assolutamente integra.

Nel caso della videosorveglianza qual è la prova che bisogna preservare? La stampa del viso incriminato, il cd su cui è stato salvato il filmato o l'hard disk? La prova, nel processo penale, è il risultato della conoscenza conseguita attraverso gli accertamenti effettuati sul mezzo di prova. Quando si tratta di indagini effettuate mediante strumenti informatici, il mezzo di prova è il dato digitale. Il reperto da acquisire è quindi il dato digitale, cioè la sequenza di uni e zeri che possono contenere informazioni attinenti all'indagine e non l'hard disk in quanto tale. E' chiaro che il dato digitale è un reperto immateriale che sussiste in quanto sussiste il mezzo che lo contiene, cioè l'hard disk.

3. "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno"

Cap. VII – PER CONCLUDERE

OCCORRE RICORDARE

a) I sistemi di videosorveglianza possono riprendere persone identificabili solo se, per raggiungere gli scopi prefissati, non possono essere utilizzati dati anonimi. Va quindi valutato se sia realmente necessario raccogliere immagini dettagliate per perseguire le finalità dichiarate.

b) La raccolta e l'uso delle immagini è consentita solo se effettuata per scopi istituzionali. Occorre valutare se la sua utilizzazione sia realmente proporzionata agli scopi perseguiti o se non sia invece superflua. Gli impianti devono cioè essere attivati solo quando altre misure siano realmente insufficienti o inattuabili.

c) Prima dell'installazione e dell'attivazione di un impianto di videosorveglianza si deve stabilire la dislocazione e la tipologia delle apparecchiature, il loro angolo visuale, l'uso di zoom automatici o di brandeggio.

d) Quando si intende installare sistemi di videosorveglianza che prevedono un intreccio delle immagini con altri particolari (es. dati biometrici,) è obbligatorio sottoporre tali sistemi alla verifica preliminare del Garante.

e) I cittadini che transitano nelle aree sorvegliate devono essere informati in modo chiaro e visibile della rilevazione delle immagini.

f) Stabilire il periodo di conservazione delle immagini a seconda delle finalità perseguite: solo per motivi di sicurezza urbana è consentita la conservazione per 7 giorni, fatte salve speciali esigenze di ulteriore conservazione in relazione a indagini.

g) Procedere alla nomina del responsabile e degli incaricati del trattamento dati

LA CARTA PER UN UTILIZZO DEMOCRATICO DELLA VIDEOSORVEGLIANZA

Una guida per le normative e le regolazioni esistenti ed un utile complemento alla gestione della videosorveglianza esercitata dalla discrezionalità delle amministrazioni pubbliche può essere rappresentata dalla Carta Europea per l'utilizzo democratico della videosorveglianza prodotta recentemente dal "*European Forum for Urban Security"* L'impiego delle telecamere di sicurezza è sempre più diffuso in Italia: ormai da una decina di anni la videosorveglianza è lo strumento tecnologico di prevenzione a cui più frequentemente fanno ricorso la amministrazioni locali, nonostante i cospicui investimenti richiesti per gestire questa strumentazione. Sono poche le ricerche orientate a valutare l'efficacia dei sistemi di videosorveglianza nella prevenzione della criminalità in termini di confronto tra costi e benefici. A livello europeo il Forum Europeo per la Sicurezza Urbana, di cui fa parte il FISU (forum italiano sicurezza urbana) al quale aderiscono molti Comuni e Regioni tra cui la Regione Piemonte. ha recentemente concluso il progetto europeo denominato «Citizens, cities and video surveillance» che, tra i prodotti ha previsto una ***carta per un utilizzo democratico della videosorveglianza.***

Il progetto «*Citizens, cities and video surveillance*», è stato finalizzato a promuovere un utilizzo ragionato delle tecnologie di controllo a distanza del territorio per la prevenzione della criminalità e ad elaborare, attraverso uno scambio di esperienze e di buone pratiche, una carta etica sul corretto utilizzo della videosorveglianza nel rispetto delle libertà individuali.

La Carta intende promuovere un uso efficace della videosorveglianza per finalità di riduzione dei comportamenti criminali con una costante attenzione ad un corretto bilanciamento tra l'esigenza di sicurezza e il rispetto della privacy dei cittadini e mira a fornire elementi di conoscenza agli operatori pubblici che possano garantire scelte equilibrate capaci di dare ai cittadini sicurezza, rispettando il loro inviolabile diritto alla riservatezza.

In sintesi, il principale vantaggio della Carta è dato dalla sua capacità di creare prassi organizzative e operative, di promuovere la responsabilità e la trasparenza, e di favorire la comprensione della videosorveglianza da parte del pubblico.

Per una lettura completa la Carta è disponibile sul sito http://cctvcharter.eu/ (versione italiana a pag 99-114).

LE LINEE GUIDA DELL'ANCI

Nel corso della XXVII Assemblea nazionale dei Comuni italiani tenutasi a Padova il 10.11.2010 sono state presentate le linee guida curate dall'Anci in collaborazione con il Garante della Privacy in materia di videosorveglianza. Il documento intende fornire chiarimenti e strumenti di lavoro per una corretta applicazione, per quanto di competenza dei Comuni, circa l'utilizzo della videosorveglianza, anche ai fini della sicurezza urbana.
Tra le numerose indicazioni degne di nota quella che consiglia ai comuni di dotarsi di un Regolamento con cui individuare le finalità e le modalità del trattamento dei dati correlato a sistemi di videoripresa. A tale scopo è l'Anci ha predisposto anche un schema tipo di Regolamento apprezzato dal Garante e che potrà facilitare molto l'attività delle amministrazioni locali.

In sintesi con tali "Linee Guida"
- viene instaurato uno stretto rapporto tra gli Uffici del Garante e l'ANCI
- vengono fornite indicazioni sulla richiesta di verifica preliminare al Garante e si chiarisce che essa va fatta solo ed esclusivamente quando l'impianto di videosorveglianza raccolga immagini associate a dati biometrici, quando permetta il riconoscimento della persona tramite confronto delle immagini rilevate (es. morfologia del volto) con altri specifici dati personali o quando si operi sulla base del confronto della relativa immagine con una campionatura di soggetti precostituita; quando l'impianto non si limiti a riprendere e registrare le immagini, ma sia in grado di rilevare automaticamente comportamenti o eventi anomali, di segnalarli, ed eventualmente di registrarli (sistemi c.d. intelligenti).
- viene indicata in maniera precisa la procedura da adottare in caso di "esame preventivo" e le motivazioni che lo rendono obbligatorio
- vengono messi in guardia i Comuni che vogliono adottare sistemi di videosorveglianza dotati di audio: sono "fuorilegge"
- vengono fornite indicazioni sull'utilizzo della videosorveglianza per finalità di "sicurezza urbana" e procedure di coinvolgimento del Comitato Provinciale per l'Ordine e la Sicurezza Pubblica, di cui fà parte il Sindaco
- si precisano le modalità di collegamento tra centrali operative delle forze di polizia e polizia locale

Da ultimo le linee guida riportano le tabelle relative alle possibili sanzioni penali e amministrative in cui potrebbero incorrere i comuni anche con riguardo alle prescrizioni del Garante.

Il documento è scaricabile dal sito:
http://www.anci.it/Contenuti/Allegati/Videosorveglianza_Web.pdf%20completo%2015%20nov.pdf

GLI ADEGUAMENTI OBBLIGATORI

Nel proprio provvedimento il Garante prescrive ai titolari del trattamento di dati personali effettuato tramite sistemi di videosorveglianza, di adottare al più presto e comunque entro e non oltre i distinti

termini di volta in volta indicati decorrenti dalla data di pubblicazione del provvedimento nella Gazzetta Ufficiale (20 aprile 2010) accorgimenti illustrati e concernenti l'obbligo di:

a) entro dodici mesi, rendere l'informativa visibile anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;

b) entro sei mesi, sottoporre i trattamenti che presentano rischi specifici per i diritti e le libertà fondamentali degli interessati, alla verifica preliminare ai sensi dell'art. 17 del Codice;

c) entro dodici mesi, adottare, le misure di sicurezza a protezione dei dati registrati tramite impianti di videosorveglianza

d) entro sei mesi, adottare le misure necessarie per garantire il rispetto delle prescrizioni specifiche in materia di sicurezza ulteriore in caso di adozione di sistemi integrati di videosorveglianza

LE SANZIONI

Le misure necessarie prescritte nel provvedimento del Garante devono essere osservate da tutti i titolari di trattamento. In caso contrario il trattamento dei dati è, a seconda dei casi, illecito oppure non corretto, ed espone:

- all'inutilizzabilità dei dati personali trattati in violazione della relativa disciplina *(art. 11, comma 2, del Codice)*;
- all'adozione di provvedimenti di blocco o di divieto del trattamento disposti dal Garante *(art. 143, comma 1, lett. c), del Codice)*, e di analoghe decisioni adottate dall'autorità giudiziaria civile e penale;
- all'applicazione delle pertinenti sanzioni amministrative o penali *(artt. 161s s. del Codice).*

Qui di seguito si indicano le principali sanzioni amministrative e penali in cui potrebbero incappare i Comuni, a seguito di visite ispettive dello specifico Nucleo Tutela Privacy del Garante per la Protezione dei Dati Personali o a seguito di segnalazioni dei cittadini, che ritengono lesa la propria riservatezza:

PRINCIPALI SANZIONI AMMINISTRATIVE (Si applicano del disposizioni della L. 689/81 - Autorità Amministrativa il Garante della Privacy – Destinatario dei proventi lo Stato)

NORMA E TIPO DI VIOLAZIONE	SANZIONE EDITTALE
Omissione o inidoneità dell'informativa (es. laddove non è indicato il titolare del trattamento o la finalità perseguita) Artt. 13 e 161 del Codice	Sanzione amm.va da 6.000 € a 36.000 €
Mancata o incompleta notificazione del trattamento dei dati personali al Garante Artt. 37, 38 e 163 del Codice	Sanzione amm.va da 20.000 € a 120.000 €
Inosservanza dei provvedimenti di prescrizione di misure necessarie Art. 162, comma 2-ter, del Codice	Sanzione amm.va da 30.000 € a 180.000 €
Omessa adozione di misure minime di sicurezza Artt. 33 e 162, comma 2-bis del Codice	Sanzione amm.va da 10.000 € a 120.000 € Non è ammesso il p.m.r.
Mancato rispetto dei tempi di conservazione delle immagini raccolte e collegato obbligo di cancellazione di delle immagini oltre il termine previsto Art. 162, comma 2-ter, del Codice	Sanzione amm.va da 30.000 € a 180.000 €
Omessa informazione o esibizione di documenti al garante Artt. 157 e 164, del Codice	Sanzione amm.va 10.000 € a 60.000 €

PRINCIPALI IPOTESI DI REATO

IPOTESI DI REATO	PENA PREVISTA
TRATTAMENTO ILLECITO DI DATI	
Trattamento illecito di dati personali da parte di soggetti pubblici (salvo che il fatto non costituisca più grave reato) Art. 167, comma 1 del Codice	Se ne deriva un danno: Reclusione da 6 mesi a 18 mesi; In caso comunicazione o diffusione dei dati: Reclusione da 6 mesi a 24 mesi
FALSITÀ NELLE DICHIARAZIONI O NOTIFICAZIONI	
Chiunque dichiari o attesti falsamente notizie o circostanze o produce atti o documenti falsi (salvo che il fatto costituisca più grave reato) Art. 168, comma 1 del Codice	Reclusione da 6 mesi a 3 anni
MISURE DI SICUREZZA	
Chiunque, essendovi tenuto, omette di adottare le misure minime di sicurezza. Art. 169, comma 1 del Codice	Arresto sino a 2 anni (reato contravvenzionale)
INOSSERVANZA DI PROVVEDIMENTI DEL GARANTE	
Chiunque, essendovi tenuto, non osserva il provvedimento del Garante Art. 170, comma 1 del Codice	Reclusione da 3 mesi a 2 anni
La condanna per uno dei delitti previsti dal D.Lgs. nr. 196 del 2003, prevede la pubblicazione della sentenza (art. 172 del Codice).	

ALLEGATO A

Provvedimento in materia di videosorveglianza - 8 aprile 2010
(Gazzetta Ufficiale n. 99 del 29 aprile 2010)

Sommario

1. Premessa

2. Trattamento dei dati personali e videosorveglianza: principi generali

3. Adempimenti applicabili a soggetti pubblici e privati

3.1. Informativa

3.1.1. Informativa e sicurezza
3.1.2. Ulteriori specificazioni: l'informativa eventuale nella videosorveglianza effettuata per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati3.1.3. Informativa da parte dei soggetti privati che effettuano collegamenti con le forze di polizia

3.2. Prescrizioni specifiche

3.2.1. Verifica preliminare
3.2.2. Esclusione della verifica preliminare
3.2.3. Notificazione

3.3. Misure di sicurezza da applicare ai dati personali trattati mediante sistemi di videosorveglianza e soggetti preposti

3.3.1. Misure di sicurezza
3.3.2. Responsabili e incaricati

3.4. Durata dell'eventuale conservazione

3.5. Diritti degli interessati

4. Settori specifici

4.1. Rapporti di lavoro

4.2. Ospedali e luoghi di cura

4.3. Istituti scolastici

4.4. Sicurezza nel trasporto pubblico

4.5. Utilizzo di web cam o camera-on-line a scopi promozionali-turistici o pubblicitari

4.6. Sistemi integrati di videosorveglianza

5. Soggetti pubblici

5.1. Sicurezza urbana

5.2. Deposito dei rifiuti

5.3. Utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada

5.4. Ulteriori avvertenze per i sistemi di videosorveglianza posti in essere da enti pubblici e, in particolare, da enti territoriali

6. Privati ed enti pubblici economici

6.1. Trattamento di dati personali per fini esclusivamente personali

6.2. Trattamento di dati personali per fini diversi da quelli esclusivamente personali

6.2.1. Consenso

6.2.2. Bilanciamento degli interessi

6.2.2.1. Videosorveglianza (con o senza registrazione delle immagini)

6.2.2.2. Riprese nelle aree condominiali comuni

7. Prescrizioni e sanzioni

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Daniele De Paoli, segretario generale reggente;

VISTO lo schema del provvedimento in materia di videosorveglianza approvato dal Garante il 22 dicembre 2009 e trasmesso al Ministero dell'Interno, all'Unione delle Province d'Italia (UPI) ed all'Associazione Nazionale Comuni Italiani (ANCI), al fine di acquisirne preventivamente le specifiche valutazioni per i profili di competenza;

CONSIDERATE le osservazioni formulate dall' ANCI con note del 25 febbraio 2010 (prot. n. 10/Area INSAP/AR/crc-10) e del 29 marzo 2010 (prot. n. 17/*Area* INSAP/AR/a*r*-10);

CONSIDERATE le osservazioni formulate dal Ministero dell'Interno con nota del 26 febbraio 2010;

VISTO il Codice in materia di protezione dei dati personali (*d.lg. 30 giugno 2003, n. 196*);

VISTE le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento n. 1/2000;

Relatore il prof. Francesco Pizzetti;

1. PREMESSA

Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza non forma oggetto di legislazione specifica; al riguardo si applicano, pertanto, le disposizioni generali in tema di protezione dei dati personali.

Il Garante ritiene necessario intervenire nuovamente in tale settore con il presente provvedimento generale che sostituisce quello del 29 aprile 2004 (1).

Ciò in considerazione sia dei numerosi interventi legislativi in materia, sia dell'ingente quantità di quesiti, segnalazioni, reclami e richieste di verifica preliminare in materia sottoposti a questa Autorità.

Nel quinquennio di relativa applicazione, infatti, talune disposizioni di legge hanno attribuito ai sindaci e ai comuni specifiche competenze volte a garantire l'incolumità pubblica e la sicurezza urbana(2), mentre altre norme, statali(3) e regionali(4), hanno previsto altresì forme di incentivazione economica a favore delle amministrazioni pubbliche e di soggetti privati al fine di incrementare l'utilizzo della videosorveglianza quale forma di difesa passiva, controllo e deterrenza di fenomeni criminosi e vandalici.

2. TRATTAMENTO DEI DATI PERSONALI E VIDEOSORVEGLIANZA: PRINCIPI GENERALI

La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali (*art. 4, comma 1, lett. b), del Codice*). È considerato dato personale, infatti, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

Un'analisi non esaustiva delle principali applicazioni dimostra che la videosorveglianza è utilizzata a fini molteplici, alcuni dei quali possono essere raggruppati nei seguenti ambiti generali:

1) 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 svolti dai soggetti pubblici, alla razionalizzazione e miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge;

2) protezione della proprietà;

3) rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge;

4) acquisizione di prove.

La necessità di garantire, in particolare, un livello elevato di tutela dei diritti e delle libertà fondamentali rispetto al trattamento dei dati personali consente la possibilità di utilizzare sistemi di videosorveglianza, purché ciò non determini un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli interessati.

Naturalmente l'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, quali ad es. le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata(5), sul controllo a distanza dei lavoratori(6), in materia di sicurezza presso stadi e impianti sportivi(7), o con riferimento a musei, biblioteche statali e archivi di Stato(8), in relazione ad impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali(9) e, ancora, nell'ambito dei porti, delle stazioni ferroviarie, delle stazioni delle ferrovie metropolitane e nell'ambito delle linee di trasporto urbano(10).

In tale quadro, pertanto, è necessario che:

a) il trattamento dei dati attraverso sistemi di videosorveglianza sia fondato su uno dei presupposti di liceità che il Codice prevede espressamente per i soggetti pubblici da un lato (svolgimento di funzioni istituzionali: *artt. 18-22 del Codice*) e, dall'altro, per soggetti privati ed enti pubblici economici (es. adempimento ad un obbligo di legge, provvedimento del Garante di c.d. "bilanciamento di interessi" -v., in proposito, punto 6.2- o consenso libero ed espresso: *artt. 23-27 del Codice*). Si tratta di presupposti operanti in settori diversi e che

sono pertanto richiamati separatamente nei successivi paragrafi del presente provvedimento relativi, rispettivamente, all'ambito pubblico e a quello privato;

b) ciascun sistema informativo ed il relativo programma informatico vengano conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (es., configurando il programma informatico in modo da consentire, per monitorare il traffico, solo riprese generali che escludano la possibilità di ingrandire le immagini e rendere identificabili le persone). Lo impone il *principio di necessità*, il quale comporta un obbligo di attenta configurazione di sistemi informativi e di programmi informatici per ridurre al minimo l'utilizzazione di dati personali (*art. 3 del Codice*);

c) l'attività di videosorveglianza venga effettuata nel rispetto del c.d. principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite (*art. 11, comma 1, lett. d) del Codice*).

3. ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI

3.1. Informativa

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti, manifestazioni sportive).

A tal fine, il Garante ritiene che si possa utilizzare lo stesso modello semplificato di informativa "minima", indicante il titolare del trattamento e la finalità perseguita, già individuato ai sensi dell'art. 13, comma 3, del Codice nel provvedimento del 2004 e riportato in *fac-simile* nell'allegato n. 1 al presente provvedimento.

Il modello è ovviamente adattabile a varie circostanze. In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, potranno essere installati più cartelli.

Il supporto con l'informativa:

• deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;

• deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;

• può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Il Garante ritiene auspicabile che l'informativa, resa in forma semplificata avvalendosi del predetto modello, poi rinvii a un testo completo contenente tutti gli elementi di cui all'art. 13, comma 1, del Codice, disponibile agevolmente senza oneri per gli interessati, con modalità facilmente accessibili anche con strumenti informatici e telematici (in particolare, tramite reti Intranet o siti Internet, affissioni in bacheche o locali, avvisi e cartelli agli sportelli per gli utenti, messaggi preregistrati disponibili digitando un numero telefonico gratuito).

In ogni caso il titolare, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dall'art. 13 del Codice.

3.1.1. Informativa e sicurezza

Talune disposizioni del Codice, tra le quali quella riguardante l'obbligo di fornire una preventiva informativa agli interessati, non sono applicabili al trattamento di dati personali effettuato, anche sotto forma di suoni e immagini, dal *"Centro elaborazione dati del Dipartimento di pubblica sicurezza o da forze di polizia sui dati destinati a confluirvi in base alla legge, ovvero da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, effettuati in base ad espressa disposizione di legge che preveda specificamente il trattamento" (art. 53 del Codice)*.

Alla luce di tale previsione del Codice, i predetti titolari del trattamento di dati personali devono osservare i seguenti principi:

a) l'informativa può non essere resa quando i dati personali sono trattati per il perseguimento delle finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati;

b) il trattamento deve comunque essere effettuato in base ad espressa disposizione di legge che lo preveda specificamente.

3.1.2. Ulteriori specificazioni: l'informativa eventuale nella videosorveglianza effettuata per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati

Il Garante, al fine di rafforzare la tutela dei diritti e delle libertà fondamentali degli interessati, ritiene fortemente auspicabile che l'informativa, benché non obbligatoria, laddove l'attività di videosorveglianza sia espletata ai sensi dell'art. 53 del Codice, sia comunque resa in tutti i casi nei quali non ostano in concreto specifiche ragioni di tutela e sicurezza pubblica o di prevenzione, accertamento o repressione dei reati.

Ciò naturalmente all'esito di un prudente apprezzamento volto a verificare che l'informativa non ostacoli, ma anzi rafforzi, in concreto l'espletamento delle specifiche funzioni perseguite, tenuto anche conto che rendere palese l'utilizzo dei sistemi di videosorveglianza può, in molti casi, svolgere una efficace funzione di deterrenza.

A tal fine i titolari del trattamento possono rendere nota la rilevazione di immagini tramite impianti di videosorveglianza attraverso forme anche semplificate di informativa, che evidenzino, mediante l'apposizione nella cartellonistica di riferimenti grafici, simboli, diciture, l'utilizzo di tali sistemi per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati.

In ogni caso resta fermo che, anche se i titolari si avvalgono della facoltà di fornire l'informativa, resta salva la non applicazione delle restanti disposizioni del Codice tassativamente indicate dall'art. 53, comma 1, lett. *a*) e *b*).

Va infine sottolineato che deve essere obbligatoriamente fornita un'idonea informativa in tutti i casi in cui, invece, i trattamenti di dati personali effettuati tramite l'utilizzo di sistemi di videosorveglianza dalle forze di polizia, dagli organi di pubblica sicurezza e da altri soggetti pubblici non siano riconducibili a quelli espressamente previsti dall'art. 53 del Codice (es. utilizzo di sistemi di rilevazioni delle immagini per la contestazione delle violazioni del Codice della strada).

3.1.3. Informativa da parte dei soggetti privati che effettuano collegamenti con le forze di polizia
I trattamenti di dati personali effettuati da soggetti privati tramite sistemi di videosorveglianza, direttamente collegati con le forze di polizia, esulano dall'ambito di applicazione dell'art. 53 del Codice. Pertanto, l'attivazione del predetto collegamento deve essere reso noto agli interessati. A tal fine, il Garante ritiene che si possa utilizzare il modello semplificato di informativa "minima" - indicante il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia- individuato ai sensi dell'art. 13, comma 3, del Codice e riportato in *fac-simile* nell'allegato n. 2 al presente provvedimento. Nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati, tale collegamento deve essere reso noto.

Al predetto trattamento si applicano le prescrizioni contenute nel punto 4.6

La violazione delle disposizioni riguardanti l'informativa di cui all'art. 13, consistente nella sua omissione o inidoneità (es. laddove non indichi comunque il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia), è punita con la sanzione amministrativa prevista dall'art. 161 del Codice.

Le diverse problematiche riguardanti le competenze attribuite ai comuni in materia di sicurezza urbana sono esaminate al punto 5.1.

3.2. Prescrizioni specifiche

3.2.1. Verifica preliminare

I trattamenti di dati personali nell'ambito di una attività di videosorveglianza devono essere effettuati rispettando le misure e gli accorgimenti prescritti da questa Autorità come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello del titolare (*art. 17 del Codice*), quando vi sono rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare.
In tali ipotesi devono ritenersi ricompresi i sistemi di raccolta delle immagini associate a dati biometrici. L'uso generalizzato e incontrollato di tale tipologia di dati può comportare, in considerazione della loro particolare natura, il concreto rischio del verificarsi di un pregiudizio rilevante per l'interessato, per cui si rende necessario prevenire eventuali utilizzi impropri, nonché possibili abusi.

Ad esempio, devono essere sottoposti alla verifica preliminare di questa Autorità i sistemi di videosorveglianza dotati di *software* che permetta il riconoscimento della persona tramite collegamento o incrocio o confronto delle immagini rilevate (es. morfologia del volto) con altri specifici dati personali, in particolare con dati biometrici, o sulla base del confronto della relativa immagine con una campionatura di soggetti precostituita alla rilevazione medesima.

Un analogo obbligo sussiste con riferimento a sistemi c.d. intelligenti, che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli. In linea di massima tali sistemi devono considerarsi eccedenti rispetto alla normale attività di videosorveglianza, in quanto possono determinare effetti particolarmente invasivi sulla sfera di autodeterminazione dell'interessato e, conseguentemente, sul suo comportamento. Il relativo utilizzo risulta comunque giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati, da verificare caso per caso sul piano della conformità ai principi di necessità, proporzionalità, finalità e correttezza (*artt. 3 e 11 del Codice*).

Deve essere sottoposto a verifica preliminare l'utilizzo di sistemi integrati di videosorveglianza nei casi in cui le relative modalità di trattamento non corrispondano a quelle individuate nei punti 4.6 e 5.4 del presente provvedimento.
Ulteriori casi in cui si rende necessario richiedere una verifica preliminare riguardano l'allungamento dei tempi di conservazione dei dati delle immagini registrate oltre il previsto termine massimo di sette giorni derivante da speciali esigenze di ulteriore conservazione, a meno che non derivi da una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria in relazione a un'attività investigativa in corso (v. punto 3.4).

Comunque, anche fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti individuati nel presente provvedimento non sono integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità.

3.2.2. Esclusione della verifica preliminare

Il titolare del trattamento di dati personali effettuato tramite sistemi di videosorveglianza non deve richiedere una verifica preliminare purché siano rispettate tutte le seguenti condizioni:

a) il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti;

b) la fattispecie concreta, le finalità del trattamento, la tipologia e le modalità d'impiego del sistema che si intende adottare, nonché le categorie dei titolari, corrispondano a quelle del trattamento approvato;

c) si rispettino integralmente le misure e gli accorgimenti conosciuti o concretamente conoscibili prescritti nel provvedimento di cui alla lett. *a*) adottato dal Garante.

Resta inteso che il normale esercizio di un impianto di videosorveglianza, non rientrante nelle ipotesi previste al precedente punto 3.2.1, non deve essere sottoposto all'esame preventivo del Garante, sempreché il trattamento medesimo avvenga con modalità conformi al presente provvedimento.

Resta altresì inteso che nessuna approvazione implicita può desumersi dal semplice inoltro al Garante di documenti relativi a progetti di videosorveglianza (spesso generici e non valutabili a distanza) cui non segua un esplicito riscontro dell'Autorità, in quanto non si applica il principio del silenzio-assenso.

3.2.3. Notificazione

E' regola generale che i trattamenti di dati personali devono essere notificati al Garante solo se rientrano in casi specificamente previsti (*art. 37 del Codice*). In relazione a quanto stabilito dalla lett. *f*), del comma 1, dell'art. 37, questa Autorità ha già disposto che non vanno comunque notificati i trattamenti di dati effettuati per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio ancorché relativi a comportamenti illeciti o fraudolenti, quando immagini o suoni raccolti siano conservati temporaneamente(11). Al di fuori di tali precisazioni, il trattamento, che venga effettuato tramite sistemi di videosorveglianza e che sia riconducibile a quanto disposto dall'art. 37 del Codice, deve essere preventivamente notificato a questa Autorità.

La mancata o incompleta notificazione ai sensi degli artt. 37 e 38 del Codice è punita con la sanzione amministrativa prevista dall'art. 163.

3.3. Misure di sicurezza da applicare ai dati personali trattati mediante sistemi di videosorveglianza e soggetti preposti

3.3.1. Misure di sicurezza

I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini (artt. 31 e ss. del Codice).

Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal titolare medesimo, nel caso in cui questo sia persona fisica).

E' inevitabile che -in considerazione dell'ampio spettro di utilizzazione di sistemi di videosorveglianza, anche in relazione ai soggetti e alle finalità perseguite nonché della varietà dei sistemi tecnologici utilizzati- le misure minime di sicurezza possano variare anche significativamente. E' tuttavia necessario che le stesse siano quanto meno rispettose dei principi che seguono:

a) in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini (v. punto 3.3.2). Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;

b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;

c) per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto (v. punto 3.4);

d) nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;

e) qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-*ter* del codice penale;

f) la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie *wi-fi, wi-max, Gprs*).

3.3.2. Responsabili e incaricati

Il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini (*art. 30 del Codice*). Deve trattarsi di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni. Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.) (v. punto 3.3.1).

Vanno osservate le regole ordinarie anche per ciò che attiene all'eventuale designazione di responsabili del trattamento (*art. 29 del Codice*).

Il mancato rispetto di quanto previsto nelle lettere da a) ad f) del punto 3.3.1 comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.

L'omessa adozione delle misure minime di sicurezza comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*bis*, ed integra la fattispecie di reato prevista dall'art. 169 del Codice.

3.4. Durata dell'eventuale conservazione

Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità (*v. art. 11, comma 1, lett. e),del Codice*), anche l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario - e predeterminato - a raggiungere la finalità perseguita.

La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, si ritiene non debba comunque superare la settimana.

Per i comuni e nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, alla luce delle recenti disposizioni normative(12), il termine massimo di durata della conservazione dei dati è limitato *"ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione"*.

In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del Garante (v. punto 3.2.1), e comunque essere ipotizzato dal titolare come eccezionale nel rispetto del principio di proporzionalità. La congruità di un termine di tempo più ampio di conservazione va adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità. La relativa congruità può altresì dipendere dalla necessità di aderire ad una specifica richiesta di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso.

Il sistema impiegato deve essere programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati. In presenza di impianti basati su tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di expiring dei dati registrati, la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal titolare.

Il mancato rispetto dei tempi di conservazione delle immagini raccolte e del correlato obbligo di cancellazione di dette immagini oltre il termine previsto comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.

3.5. Diritti degli interessati

Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al Codice, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento (*art. 7 del Codice*).

La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti al richiedente identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal Codice, ovvero nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato (*art. 10, comma 5, del Codice*).

In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo (*art. 7, comma 3, lett. a), del Codice*). Viceversa, l'interessato ha diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge (*art. 7, comma 3, lett. b), del Codice*).

4. SETTORI SPECIFICI

4.1. Rapporti di lavoro

Nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa, pertanto è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul *badge*). Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell'art. 4 della l. n. 300/1970, gli impianti e le apparecchiature, "*dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti" (v., altresì, artt. 113 e 114 del Codice; art. 8 l. n. 300/1970 cit.; art. 2 d.lg. n. 165/2001).*

Tali garanzie vanno osservate sia all'interno degli edifici, sia in altri contesti in cui è resa la prestazione di lavoro, come, ad esempio, nei cantieri edili o con riferimento alle telecamere installate su veicoli adibiti al servizio di linea per il trasporto di persone (artt. 82, 85-87, d.lg. 30 aprile 1992, n. 285, "*Nuovo codice della strada*") o su veicoli addetti al servizio di noleggio con conducente e servizio di piazza (taxi) per trasporto di persone (le quali non devono riprendere in modo stabile la postazione di guida, e le cui immagini, raccolte per finalità di sicurezza e di eventuale accertamento di illeciti, non possono essere utilizzate per controlli, anche indiretti, sull'attività lavorativa degli addetti, v. punto 4.4).

Il mancato rispetto di quanto sopra prescritto comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.

L'utilizzo di sistemi di videosorveglianza preordinati al controllo a distanza dei lavoratori o ad effettuare indagini sulle loro opinioni integra la fattispecie di reato prevista dall'art. 171 del Codice.

Sotto un diverso profilo, eventuali riprese televisive sui luoghi di lavoro per documentare attività od operazioni solo per scopi divulgativi o di comunicazione istituzionale o aziendale, e che vedano coinvolto il personale dipendente, possono essere assimilati ai trattamenti temporanei finalizzati alla pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull'attività giornalistica contenute nel Codice (*artt. 136 e ss.*), fermi restando, comunque, i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l'osservanza del codice deontologico per l'attività giornalistica ed il diritto del lavoratore a tutelare la propria immagine opponendosi, per motivi legittimi, alla sua diffusione (*art. 7, comma 4, lett. a), del Codice*).

4.2. Ospedali e luoghi di cura

L'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (ad es. unità di rianimazione, reparti di isolamento), stante la natura sensibile di molti dati che possono essere in tal modo raccolti, devono essere limitati ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute degli interessati.

Devono essere inoltre adottati tutti gli ulteriori accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate, anche in attuazione di quanto prescritto dal provvedimento generale del 9 novembre 2005 adottato in attuazione dell'art. 83 del Codice(13).

Il titolare deve garantire che possano accedere alle immagini rilevate per le predette finalità solo i soggetti specificamente autorizzati (es. personale medico ed infermieristico). Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di terzi legittimati (familiari, parenti, conoscenti) di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione), ai quali

può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto o conoscente.

Le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse (*art. 22, comma 8, del Codice*). In tale quadro, va assolutamente evitato il rischio di diffusione delle immagini di persone malate su *monitor* collocati in locali liberamente accessibili al pubblico.

Il mancato rispetto di quanto sopra prescritto comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.

La diffusione di immagini in violazione dell'art. 22, comma 8, del Codice, oltre a comportare l'applicazione della sanzione amministrativa prevista dall'art. 162, comma 2-*bis*, integra la fattispecie di reato stabilita dall'art. 167, comma 2.

4.3. Istituti scolastici

L'eventuale installazione di sistemi di videosorveglianza presso istituti scolastici deve garantire *"il diritto dello studente alla riservatezza"* (*art. 2, comma 2, d.P.R. n. 249/1998*), prevedendo opportune cautele al fine di assicurare l'armonico sviluppo delle personalità dei minori in relazione alla loro vita, al loro processo di maturazione ed al loro diritto all'educazione(14).

4.3.1. In tale quadro, può risultare ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate ed attivando gli impianti negli orari di chiusura degli istituti; è vietato, altresì, attivare le telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche che si svolgono all'interno della scuola.

4.3.2. Laddove la ripresa delle immagini riguardi anche le aree perimetrali esterne degli edifici scolastici, l'angolo visuale deve essere delimitato alle sole parti interessate, escludendo dalle riprese le aree non strettamente pertinenti l'edificio.

4.3.3. Il mancato rispetto di quanto prescritto ai punti 4.3.1 e 4.3.2 comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-ter, del Codice.

4.4. Sicurezza nel trasporto pubblico

4.4.1. Alcune situazioni di particolare rischio possono fare ritenere lecita l'installazione di sistemi di videosorveglianza sia su mezzi di trasporto pubblici, sia presso le fermate dei predetti mezzi.

4.4.2. La localizzazione delle telecamere e le modalità di ripresa devono essere determinate nel rispetto dei richiamati principi di necessità, proporzionalità e finalità; pertanto, occorre evitare riprese particolareggiate nei casi in cui le stesse non sono indispensabili in relazione alle finalità perseguite.

4.4.3. I titolari del trattamento dovranno poi provvedere a fornire la prevista informativa agli utenti del servizio di trasporto urbano. Gli autobus, i tram, i taxi ed i veicoli da noleggio con o senza conducente dotati di telecamere dovranno pertanto portare apposite indicazioni o contrassegni che diano conto con immediatezza della presenza dell'impianto di videosorveglianza, anche utilizzando a tal fine il *fac-simile* riportato nell'allegato n. 1 al presente provvedimento, e indicanti, comunque, il titolare del trattamento, nonché la finalità perseguita.

4.4.4. Specifiche cautele devono essere osservate laddove vengano installati impianti di videosorveglianza presso le aree di fermata, in prossimità delle quali possono transitare anche soggetti diversi dagli utenti del servizio di trasporto pubblico. In particolare, l'angolo visuale delle apparecchiature di ripresa deve essere strettamente circoscritto all'area di permanenza, permettendo l'inquadratura solo della pensilina e di altri

arredi urbani funzionali al servizio di trasporto pubblico (tabelle degli orari, paline recanti l'indicazione degli autobus in transito, ecc.), con esclusione della zona non immediatamente circostante e comunque dell'area non direttamente funzionale rispetto alle esigenze di sicurezza del sistema di traffico e trasporto. Anche in tale ipotesi occorre evitare le riprese inutilmente particolareggiate o tali da rilevare caratteristiche eccessivamente dettagliate degli individui che stazionano presso le fermate. L'esistenza delle telecamere deve essere opportunamente evidenziata nelle predette aree di fermata.

4.4.5. Fermo restando che la violazione delle disposizioni riguardanti l'informativa di cui all'art. 13 è punita con la sanzione amministrativa prevista dall'art. 161 del Codice e l'utilizzo di sistemi di videosorveglianza preordinati al controllo a distanza dei lavoratori integra la fattispecie di reato prevista dall'art. 171, il mancato rispetto di quanto prescritto al punto 4.4.4 comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.

4.5. Utilizzo di web cam o camera-on-line a scopi promozionali-turistici o pubblicitari
Le attività di rilevazione di immagini a fini promozionali-turistici o pubblicitari, attraverso *web cam* devono avvenire con modalità che rendano non identificabili i soggetti ripresi. Ciò in considerazione delle peculiari modalità del trattamento, dalle quali deriva un concreto rischio del verificarsi di un pregiudizio rilevante per gli interessati: le immagini raccolte tramite tali sistemi, infatti, vengono inserite direttamente sulla rete Internet, consentendo a chiunque navighi sul web di visualizzare in tempo reale i soggetti ripresi e di utilizzare le medesime immagini anche per scopi diversi dalle predette finalità promozionali-turistiche o pubblicitarie perseguite dal titolare del trattamento.

4.6. Sistemi integrati di videosorveglianza

In ottemperanza del principio di economicità delle risorse e dei mezzi impiegati, si è incrementato il ricorso a sistemi integrati di videosorveglianza tra diversi soggetti, pubblici e privati, nonché l'offerta di servizi centralizzati di videosorveglianza remota da parte di fornitori (società di vigilanza, *Internet service providers*, fornitori di servizi video specialistici, ecc.). Inoltre, le immagini riprese vengono talvolta rese disponibili, con varie tecnologie o modalità, alle forze di polizia.

Nell'ambito dei predetti trattamenti, sono individuabili le seguenti tipologie di sistemi integrati di videosorveglianza:

a) *gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento*, i quali utilizzano le medesime infrastrutture tecnologiche; in tale ipotesi, i singoli titolari possono trattare le immagini solo nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali ed alle finalità chiaramente indicate nell'informativa, nel caso dei soggetti pubblici, ovvero alle sole finalità riportate nell'informativa, nel caso dei soggetti privati;

b) *collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo*; tale soggetto terzo, designato responsabile del trattamento ai sensi dell'art. 29 del Codice da parte di ogni singolo titolare, deve assumere un ruolo di coordinamento e gestione dell'attività di videosorveglianza senza consentire, tuttavia, forme di correlazione delle immagini raccolte per conto di ciascun titolare;

c) sia nelle predette ipotesi, sia nei casi in cui l'attività di videosorveglianza venga effettuata da un solo titolare, si può anche attivare un *collegamento dei sistemi di videosorveglianza con le sale o le centrali operative degli organi di polizia*. L'attivazione del predetto collegamento deve essere reso noto agli interessati. A tal fine, il Garante ritiene che si possa utilizzare il modello semplificato di informativa "minima" - indicante il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia- individuato ai sensi dell'art. 13, comma 3, del Codice e riportato in *fac-simile* nell'allegato n. 2 al presente provvedimento. Tale collegamento deve essere altresì reso noto nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati (v. punto 3.1.3).

Le modalità di trattamento sopra elencate richiedono l'adozione di specifiche misure di sicurezza ulteriori rispetto a quelle individuate nel precedente punto 3.3.1, quali:

1) adozione di sistemi idonei alla registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei responsabili da parte del titolare, comunque non inferiore a sei mesi;

2) separazione logica delle immagini registrate dai diversi titolari.
Il mancato rispetto delle misure previste ai punti 1) e 2) comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.
Fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità (v. punto 3.2.1).

5. SOGGETTI PUBBLICI

I soggetti pubblici, in qualità di titolari del trattamento (*art. 4, comma 1, lett. f), del Codice*), possono trattare dati personali nel rispetto del principio di finalità, perseguendo scopi determinati, espliciti e legittimi (*art. 11, comma 1, lett. b), del Codice*), soltanto per lo svolgimento delle proprie funzioni istituzionali. Ciò vale ovviamente anche in relazione a rilevazioni di immagini mediante sistemi di videosorveglianza (*art. 18, comma 2, del Codice*).

I soggetti pubblici sono tenuti a rispettare, al pari di ogni titolare di trattamento effettuato tramite sistemi di videosorveglianza, i principi enunciati nel presente provvedimento.

Anche per i soggetti pubblici sussiste l'obbligo di fornire previamente l'informativa agli interessati (*art. 13 del Codice*), ferme restando le ipotesi prese in considerazione al punto 3.1.1. Pertanto, coloro che accedono o transitano in luoghi dove sono attivi sistemi di videosorveglianza devono essere previamente informati in ordine al trattamento dei dati personali. A tal fine, anche i soggetti pubblici possono utilizzare il modello semplificato di informativa "minima", riportato in *fac-simile* nell'allegato n. 1 al presente provvedimento (v. punto 3.1).

5.1. Sicurezza urbana

Recenti disposizioni legislative in materia di sicurezza hanno attribuito ai sindaci il compito di sovrintendere alla vigilanza ed all'adozione di atti che sono loro attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica, nonché allo svolgimento delle funzioni affidati ad essi dalla legge in materia di sicurezza e di polizia giudiziaria(15). Al fine di prevenire e contrastare determinati pericoli(16) che minacciano l'incolumità pubblica e la sicurezza urbana, il sindaco può altresì adottare provvedimenti, anche contingibili e urgenti, nel rispetto dei principi generali dell'ordinamento. Infine, il sindaco, quale ufficiale del Governo, concorre ad assicurare la cooperazione della polizia locale con le forze di polizia statali, nell'ambito delle direttive di coordinamento impartite dal Ministero dell'interno.

Da tale quadro emerge che sussistono specifiche funzioni attribuite sia al sindaco, quale ufficiale del Governo, sia ai comuni, rispetto alle quali i medesimi soggetti possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico al fine di tutelare la sicurezza urbana(17).

Non spetta a questa Autorità definire il concetto di sicurezza urbana e delimitarne l'ambito operativo rispetto a quelli di ordine e sicurezza pubblica; purtuttavia, resta inteso che, nelle ipotesi in cui le attività di videosorveglianza siano assimilabili alla tutela della sicurezza pubblica, nonché alla prevenzione, accertamento o repressione dei reati, trova applicazione l'art. 53 del Codice (v. punto 3.1.1).

In ogni caso, si ribadisce l'auspicio che, nelle predette ipotesi, l'informativa, benché non obbligatoria, venga comunque resa, specie laddove i comuni ritengano opportuno rendere noto alla cittadinanza l'adozione di misure e accorgimenti, quali l'installazione di sistemi di videosorveglianza, volti al controllo del territorio e alla protezione degli individui.

5.2. Deposito dei rifiuti

In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi.

Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (art. 13, l. 24 novembre 1981, n. 689).

5.3. Utilizzo di dispositivi elettronici per la rilevazione di violazioni al Codice della strada
Gli impianti elettronici di rilevamento automatizzato delle infrazioni, utilizzati per documentare la violazione delle disposizioni in materia di circolazione stradale, analogamente all'utilizzo di sistemi di videosorveglianza, comportano un trattamento di dati personali.

5.3.1. L'utilizzo di tali sistemi è quindi lecito se sono raccolti solo dati pertinenti e non eccedenti per il perseguimento delle finalità istituzionali del titolare, delimitando a tal fine la dislocazione e l'angolo visuale delle riprese in modo da non raccogliere immagini non pertinenti o inutilmente dettagliate. In conformità alla prassi ed al quadro normativo di settore riguardante talune violazioni del Codice della strada(18), il Garante prescrive quanto segue:

a) gli impianti elettronici di rilevamento devono circoscrivere la conservazione dei dati alfanumerici contenuti nelle targhe automobilistiche ai soli casi in cui risultino non rispettate le disposizioni in materia di circolazione stradale;

b) le risultanze fotografiche o le riprese video possono individuare unicamente gli elementi previsti dalla normativa di settore per la predisposizione del verbale di accertamento delle violazioni (*es., ai sensi dell'art. 383 del d.P.R. n. 495/1992, il tipo di veicolo, il giorno, l'ora e il luogo nei quali la violazione è avvenuta*); deve essere effettuata una ripresa del veicolo che non comprenda o, in via subordinata, mascheri, per quanto possibile, la porzione delle risultanze video/fotografiche riguardanti soggetti non coinvolti nell'accertamento amministrativo (es., pedoni, altri utenti della strada);

c) le risultanze fotografiche o le riprese video rilevate devono essere utilizzate solo per accertare le violazioni delle disposizioni in materia di circolazione stradale anche in fase di contestazione, ferma restando la loro accessibilità da parte degli aventi diritto;

d) le immagini devono essere conservate per il periodo di tempo strettamente necessario in riferimento alla contestazione, all'eventuale applicazione di una sanzione e alla definizione del possibile contenzioso in conformità alla normativa di settore(19), fatte salve eventuali esigenze di ulteriore conservazione derivanti da una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria;

e) le fotografie o le immagini che costituiscono fonte di prova per le violazioni contestate non devono essere inviate d'ufficio al domicilio dell'intestatario del veicolo unitamente al verbale di contestazione, ferma restando la loro accessibilità agli aventi diritto;

f) in considerazione del legittimo interesse dell'intestatario del veicolo di verificare l'autore della violazione e, pertanto, di ottenere dalla competente autorità ogni elemento a tal fine utile, la visione della documentazione video-fotografica deve essere resa disponibile a richiesta del destinatario del verbale; al

momento dell'accesso, dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo.

Il mancato rispetto di quanto sopra prescritto nelle lettere da a) ad f) comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-ter, del Codice.

5.3.2. Anche i conducenti dei veicoli e le persone che accedono o transitano in aree dove sono attivi sistemi elettronici di rilevazione automatizzata delle violazioni devono essere previamente informati in ordine al trattamento dei dati personali (*art. 13 del Codice*).
Particolari disposizioni normative vigenti individuano già talune ipotesi (come, ad es., in caso di rilevamento a distanza dei limiti di velocità) in cui l'amministrazione pubblica è tenuta a informare gli utenti in modo specifico in ordine all'utilizzo di dispositivi elettronici(20).

L'obiettivo da assicurare è quello di un'efficace informativa agli interessati, che può essere fornita dagli enti preposti alla rilevazione delle immagini attraverso più soluzioni.

Un'idonea informativa in materia può essere anzitutto assicurata mediante l'utilizzo di strumenti appropriati che rendano agevolmente conoscibile l'esistenza e la presenza nelle aree interessate degli strumenti di rilevamento di immagini. A tal fine, svolgono un ruolo efficace gli strumenti di comunicazione al pubblico e le iniziative periodiche di diffusa informazione (*siti web*, comunicati scritti); tali forme di informazione possono essere eventualmente integrate con altre modalità (es., volantini consegnati all'utenza, pannelli a messaggio variabile, annunci televisivi e radiofonici, reti civiche e altra comunicazione istituzionale).

A integrazione di tali strumenti di comunicazione e informazione, va considerato il contributo che possono dare appositi cartelli. A tal fine, il modello semplificato di informativa "minima", riportato nel *fac-simile* in allegato, può essere utilizzato nei casi in cui la normativa in materia di circolazione stradale non prevede espressamente l'obbligo di informare gli utenti relativamente alla presenza di dispositivi elettronici volti a rilevare automaticamente le infrazioni.

Come si è detto, la normativa di settore prevede espressamente, in alcuni casi (es., rilevamento a distanza dei limiti di velocità, dei sorpassi vietati), l'obbligo di rendere nota agli utenti l'installazione degli impianti elettronici di rilevamento automatizzato delle infrazioni. In questi stessi casi è quindi possibile fare a meno di fornire un'ulteriore, distinta informativa rispetto al trattamento dei dati che riproduca gli elementi che sono già noti agli interessati per effetto degli avvisi di cui alla disciplina di settore in tema di circolazione stradale (*art. 13, comma 2, del Codice*). L'installazione di questi ultimi appositi avvisi previsti dal Codice della strada permette già agli interessati di percepire vari elementi essenziali in ordine al trattamento dei propri dati personali. Pertanto, gli avvisi che segnalano adeguatamente l'attivazione di dispositivi elettronici di rilevazione automatica delle infrazioni possono essere considerati idonei ad adempiere all'obbligo di fornire l'informativa di cui all'art. 13 del Codice.

Infine, l'obbligo di fornire tale informativa deve ritenersi soddisfatto anche quando il titolare del trattamento, pur mancando una previsione normativa che obblighi specificamente a segnalare la rilevazione automatizzata, la segnali comunque utilizzando avvisi analoghi a quelli previsti dal Codice della strada.

La violazione delle disposizioni riguardanti l'informativa di cui all'art. 13 è punita con la sanzione amministrativa prevista dall'art. 161 del Codice.

5.3.3. Qualora si introducano sistemi di rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato, i comuni dovranno rispettare quanto previsto dal d.P.R. 22 giugno 1999, n. 250. Tale normativa prevede che i dati trattati possono essere conservati solo per il periodo necessario per contestare le infrazioni e definire il relativo contenzioso, ferma restando l'accessibilità agli stessi per fini di polizia giudiziaria o di indagine penale (*art. 3 d.P.R. n. 250/1999*).

5.4. Ulteriori avvertenze per i sistemi di videosorveglianza posti in essere da enti pubblici e, in particolare, da enti territoriali

Anche gli enti territoriali e, in generale, i soggetti pubblici operanti sul territorio effettuano attività di videosorveglianza in forma integrata, tramite la compartecipazione ad un medesimo sistema di rilevazione, al fine di economizzare risorse e mezzi impiegati nell'espletamento delle più diverse attività istituzionali.

Questa Autorità ha già individuato al punto 4.6 un quadro di specifiche garanzie in ordine alle corrette modalità che vengono qui ulteriormente richiamate, in particolare con riferimento all'attività del controllo sul territorio da parte dei comuni, anche relativamente a quanto disposto in materia di videosorveglianza comunale(21).

In particolare:

a) l'utilizzo condiviso, in forma integrale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica deve essere configurato con modalità tali da permettere ad ogni singolo ente e, in taluni casi, anche alle diverse strutture organizzative dell'ente, l'accesso alle immagini solo nei termini strettamente funzionali allo svolgimento dei propri compiti istituzionali, evitando di tracciare gli spostamenti degli interessati e di ricostruirne il percorso effettuato in aree che esulano dalla competenza territoriale dell'ente;

b) nei casi in cui un "centro" unico gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici, i dati personali raccolti dovranno essere trattati in forma differenziata e rigorosamente distinta, in relazione alle competenze istituzionali della singola pubblica amministrazione.

Il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità fuori dalle predette ipotesi, ed in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento, agli effetti che possono determinare o, a maggior ragione, con riferimento a quei sistemi per i quali già il punto 3.2.1 la richiede (es. sistemi di raccolta delle immagini associate a dati biometrici o c.d. intelligenti, cioè in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli).

6. PRIVATI ED ENTI PUBBLICI ECONOMICI

6.1. Trattamento di dati personali per fini esclusivamente personali

L'installazione di sistemi di videosorveglianza -come si rileva dall'esame di numerose istanze pervenute all'Autorità- viene sovente effettuata da persone fisiche per fini esclusivamente personali. In tal caso va chiarito che la disciplina del Codice non trova applicazione qualora i dati non siano comunicati sistematicamente a terzi ovvero diffusi, risultando comunque necessaria l'adozione di cautele a tutela dei terzi (*art. 5, comma 3*, del Codice, che fa salve le disposizioni in tema di responsabilità civile e di sicurezza dei dati). In tali ipotesi possono rientrare, a titolo esemplificativo, strumenti di videosorveglianza idonei ad identificare coloro che si accingono ad entrare in luoghi privati (videocitofoni ovvero altre apparecchiature che rilevano immagini o suoni, anche tramite registrazione), oltre a sistemi di ripresa installati nei pressi di immobili privati ed all'interno di condomini e loro pertinenze (quali posti auto e *box*).

Benché non trovi applicazione la disciplina del Codice, al fine di evitare di incorrere nel reato di interferenze illecite nella vita privata (*art. 615-bis c.p.*), l'angolo visuale delle riprese deve essere comunque limitato ai soli spazi di propria esclusiva pertinenza (ad esempio antistanti l'accesso alla propria abitazione) escludendo ogni forma di ripresa, anche senza registrazione di immagini, relativa ad aree comuni (cortili, pianerottoli, scale, garage comuni) ovvero ad ambiti antistanti l'abitazione di altri condomini.

6.2. Trattamento di dati personali per fini diversi da quelli esclusivamente personali

6.2.1. Consenso

Nel caso in cui trovi applicazione la disciplina del Codice, il trattamento di dati può essere lecitamente effettuato da privati ed enti pubblici economici solamente se vi sia il consenso preventivo dell'interessato, oppure se ricorra uno dei presupposti di liceità previsti in alternativa al consenso (*artt. 23 e 24 del Codice*).

Nel caso di impiego di strumenti di videosorveglianza la possibilità di acquisire il consenso risulta in concreto limitata dalle caratteristiche stesse dei sistemi di rilevazione che rendono pertanto necessario individuare un'idonea alternativa nell'ambito dei requisiti equipollenti del consenso di cui all'art. 24, comma 1, del Codice.

6.2.2. Bilanciamento degli interessi

Tale alternativa può essere ravvisata nell'istituto del bilanciamento di interessi (*art. 24, comma 1, lett. g), del Codice*). Il presente provvedimento dà attuazione a tale istituto, individuando i casi in cui la rilevazione delle immagini può avvenire senza consenso, qualora, con le modalità stabilite in questo stesso provvedimento, sia effettuata nell'intento di perseguire un legittimo interesse del titolare o di un terzo attraverso la raccolta di mezzi di prova o perseguendo fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, o finalità di prevenzione di incendi o di sicurezza del lavoro.

A tal fine, possono essere individuati i seguenti casi, in relazione ai quali, con le precisazioni di seguito previste, il trattamento può lecitamente avvenire pure in assenza del consenso.

6.2.2.1. Videosorveglianza (con o senza registrazione delle immagini)

Tali trattamenti sono ammessi in presenza di concrete situazioni che giustificano l'installazione, a protezione delle persone, della proprietà o del patrimonio aziendale.

Nell'uso delle apparecchiature volte a riprendere, con o senza registrazione delle immagini, aree esterne ad edifici e immobili (perimetrali, adibite a parcheggi o a carico/scarico merci, accessi, uscite di emergenza), resta fermo che il trattamento debba essere effettuato con modalità tali da limitare l'angolo visuale all'area effettivamente da proteggere, evitando, per quanto possibile, la ripresa di luoghi circostanti e di particolari che non risultino rilevanti (vie, edifici, esercizi commerciali, istituzioni ecc.).

6.2.2.2. Riprese nelle aree condominiali comuni

Qualora i trattamenti siano effettuati dal condominio (anche per il tramite della relativa amministrazione), si evidenzia che tale specifica ipotesi è stata recentemente oggetto di una segnalazione da parte del Garante al Governo ed al Parlamento(22); ciò in relazione all'assenza di una puntuale disciplina che permetta di risolvere alcuni problemi applicativi evidenziati nell'esperienza di questi ultimi anni. Non è infatti chiaro se l'installazione di sistemi di videosorveglianza possa essere effettuata in base alla sola volontà dei comproprietari, o se rilevi anche la qualità di conduttori. Non è parimenti chiaro quale sia il numero di voti necessario per la deliberazione condominiale in materia (se occorra cioè l'unanimità ovvero una determinata maggioranza).

7. PRESCRIZIONI E SANZIONI

Il Garante invita tutti i titolari dei trattamenti di dati personali effettuati tramite sistemi di videosorveglianza ad attenersi alle prescrizioni indicate nel presente provvedimento.

Le misure necessarie prescritte con il presente provvedimento devono essere osservate da tutti i titolari di trattamento. In caso contrario il trattamento dei dati è, a seconda dei casi, illecito oppure non corretto, ed espone:

• all'inutilizzabilità dei dati personali trattati in violazione della relativa disciplina (*art. 11, comma 2, del Codice*);

• all'adozione di provvedimenti di blocco o di divieto del trattamento disposti dal Garante (*art. 143, comma 1, lett. c*), del Codice), e di analoghe decisioni adottate dall'autorità giudiziaria civile e penale;

• all'applicazione delle pertinenti sanzioni amministrative o penali (*artt. 161 e ss. del Codice*).

TUTTO CIÒ PREMESSO IL GARANTE:

1. prescrive ai sensi dell'art. 154, comma 1, lett. c), del Codice, ai titolari del trattamento di dati personali effettuato tramite sistemi di videosorveglianza, di adottare al più presto e, comunque, entro e non oltre i distinti termini di volta in volta indicati decorrenti dalla data di pubblicazione del presente provvedimento nella Gazzetta Ufficiale della Repubblica italiana, le misure e gli accorgimenti illustrati in premessa e di seguito individuati concernenti l'obbligo di:

a) entro dodici mesi, rendere l'informativa visibile anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno (punto 3.1);

b) entro sei mesi, sottoporre i trattamenti che presentano rischi specifici per i diritti e le libertà fondamentali degli interessati, alla verifica preliminare ai sensi dell'art. 17 del Codice (punto 3.2.1);

c) entro dodici mesi, adottare, le misure di sicurezza a protezione dei dati registrati tramite impianti di videosorveglianza (punto 3.3);

d) entro sei mesi, adottare le misure necessarie per garantire il rispetto di quanto indicato nei punti 4.6 e 5.4, per quanto concerne i sistemi integrati di videosorveglianza;

2. individua, nei termini di cui in motivazione, ai sensi dell'art. 24, comma 1, lett. *g*), del Codice, i casi nei quali il trattamento dei dati personali mediante videosorveglianza può essere effettuato da soggetti privati ed enti pubblici economici, nei limiti e alle condizioni indicate, per perseguire legittimi interessi e senza richiedere il consenso degli interessati (punto 6.2.2);

3. individua nell'allegato 1, ai sensi dell'art. 13, comma 3, del Codice, un modello semplificato di informativa utilizzabile alle condizioni indicate in motivazione (punto 3.1);

4. individua nell'allegato 2, ai sensi dell'art. 13, comma 3, del Codice, un modello semplificato di informativa utilizzabile alle condizioni indicate in motivazione, al fine di rendere noto agli interessati l'attivazione di un collegamento del sistema di videosorveglianza con le forze di polizia (punti 3.1.3 e 4.6, lett. c));

5. segnala l'opportunità che, anche nell'espletamento delle attività di cui all'art. 53 del Codice, l'informativa, benché non obbligatoria, sia comunque resa in tutti i casi nei quali non ostano in concreto specifiche ragioni di tutela e sicurezza pubblica o di prevenzione, accertamento o repressione dei reati (punto 5.1);

6. dispone, ai sensi dell'art. 143, comma 2, del Codice, che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 8 aprile 2010

IL PRESIDENTE
F.to Pizzetti

IL RELATORE
F.to Pizzetti

IL SEGRETARIO GENERALE REGGENTE
F.to De Paoli

ALLEGATO B

SCHEMA DI NUOVO REGOLAMENTO PER LA DISCIPLINA DELLA VIDEOSORVEGLIANZA NEL TERRITORIO COMUNALE DI …….. AGGIORNAMENTO 2010
(Approvato con deliberazione di C.C. N° …. del …….)

Tratto dalla pubblicazione: "Linee Guida per i Comuni in materia di Videosorveglianza alla luce del Provvedimento del Garante della Privacy dell' 8 aprile 2010" curata dall'ANCI

INDICE

CAPO I
PRINCIPI GENERALI

Art. 1 - Oggetto
Art. 2 - Definizioni
Art. 3 - Finalità
Art. 4 - Trattamento dei dati personali

CAPO II
OBBLIGHI PER IL TITOLARE DEL TRATTAMENTO

Art. 5 - Notificazione
Art. 6 - Responsabile
Art. 7 - Persone autorizzate ad accedere alla sala di controllo
Art. 8 - Nomina degli incaricati e dei preposti gestione dell'impianto di videosorveglianza
Art. 9 - Accesso ai sistemi e parola chiave

CAPO III
TRATTAMENTO DEI DATI PERSONALI

Sezione I – Raccolta e requisiti dei dati personali
Art. 10 - Modalità di raccolta e requisiti dei dati personali
Art. 11 - Obbligo degli operatori
Art. 12 - Informazioni rese al momento della raccolta

Sezione II – Diritti dell'interessato nel trattamento dei dati
Art. 13 - Diritti dell'interessato

Sezione III – Sicurezza nel trattamento dei dati, limiti alla utilizzabilità dei dati e risarcimento dei danni
Art. 14 - Sicurezza dei dati
Art. 15 - Cessazione del trattamento dei dati
Art. 16 - Limiti alla utilizzazione di dati personali
Art. 17 - Danni cagionati per effetto del trattamento di dati personali

Sezione IV – Comunicazione e diffusione dei dati
Art. 18 - Comunicazione

CAPO IV
TUTELA AMMINISTRATIVA E GIURISDIZIONALE
Art. 19 - Tutela

CAPO V
MODIFICHE
Art. 20 - Modifiche regolamentari

CAPO I
PRINCIPI GENERALI

Art. 1 – Oggetto e norme di riferimento

1. Il presente regolamento disciplina il trattamento dei dati personali, realizzato mediante l'impianto di videosorveglianza cittadina, attivato nel territorio urbano del Comune di.-----

2. Per tutto quanto non è dettagliatamente disciplinato nel presente regolamento, si rinvia a quanto disposto dal lCodice in materia di protezione dei dati personali approvato con Decreto Legislativo 30 giugno 2003, n. 196 e al Provvedimento Garante Privacy in materia di videosorveglianza 8 aprile 2010.

3. Vengono osservate i principi dal Regolamento sulla videosorveglianza del 2004, circolare Capo della Polizia nr. 558/A/421.2/70/456 del febbraio 2005, circolare del Capo della Polizia nr. 558/A/421.2/70/195960 del 6 agosto 2010.

ART. 2 – Definizioni

1. Ai fini del presente regolamento si intende:
a) per "**banca dati**", il complesso di dati personali, formatosi presso la sala di controllo e trattato esclusivamente mediante riprese video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto;
b) per "**trattamento**", tutte le operazioni o complesso di operazioni, svolte con l'ausilio dei mezzi elettronici, informatici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, l'eventuale diffusione, la cancellazione e la distribuzione di dati;
c) per "**dato personale**", qualunque informazione relativa a persona fisica, persona giuridica, Ente o associazione, identificati o identificabili anche direttamente, e rilevati con trattamenti di immagini effettuati attraverso l'impianto di videosorveglianza;
d) per "**titolare**", l'Ente Comune di -------, nelle sue articolazioni interne, cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali;
e) per "**responsabile**", la persona fisica, legata da rapporto di servizio al titolare e preposto dal medesimo al trattamento dei dati personali;
f) per "**incaricat**i", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
g) per "**interessato**", la persona fisica, la persona giuridica, l'Ente o associazione cui si riferiscono i dati personali;
h) per "**comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
i) per "**diffusione**", il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
l) per "**dato anonimo**", il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
m) per "**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.

ART. 3 – Finalità

1. Il presente regolamento garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di un impianto di videosorveglianza nel territorio urbano, gestito dal Comune di --- - Corpo di Polizia Municipale e collegato alla centrale operativa della stessa Polizia Municipale nonché a quella della Questura di ----, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. Garantisce, altresì, i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento. Il sistema informativo e i programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzati mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

2. Presso la centrale operativa della Polizia Municipale e della Questura sono posizionati monitor per la visione in diretta delle immagini riprese dalle telecamere.

Art. 4 - Trattamento dei dati personali

1. Il trattamento dei dati personali è effettuato a seguito dell'attivazione di un impianto di videosorveglianza.

2. Le finalità istituzionali del suddetto impianto sono del tutto conformi alle funzioni istituzionali demandate al Comune di ----, in particolare dal D.lgs.18 agosto 2000 n. 267, dal D.P.R. 24 luglio 1977, n.616, dal D.Lgs.31 marzo 1998, dalla legge 7 marzo 1986 n. 65, sull'ordinamento della Polizia Municipale, nonché dallo statuto e dai regolamenti comunali.
La disponibilità tempestiva di immagini presso il Comando della Polizia Municipale e della Questura di ---- costituisce, inoltre, uno strumento di prevenzione e di razionalizzazione dell'azione delle pattuglie della Polizia Municipale e della Polizia di Stato sul territorio comunale, in stretto raccordo con le altre forze dell'ordine.

3. Gli impianti di videosorveglianza, in sintesi, sono finalizzati:
a) a prevenire e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e quindi ad assicurare maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana", cos' individuata secondo il Decreto Ministro Interno 5 agosto 2008;
b) a tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale e a prevenire eventuali atti di vandalismo o danneggiamento;
c) al controllo di determinate aree;
d) al monitoraggio del traffico;
e) tutelando in tal modo coloro che più necessitano di attenzione: bambini, giovani e anziani, garantendo un elevato grado di sicurezza nelle zone monitorate.

4. Il sistema di videosorveglianza comporterà esclusivamente il trattamento di dati personali rilevati mediante le riprese video e che, in relazione ai luoghi di installazione delle videocamere, interessano i soggetti ed i mezzi di trasporto che transiteranno nell'area interessata.

5. Gli impianti di videosorveglianza non potranno essere utilizzati, in base all'art. 4 dello statuto dei lavoratori (legge 300 del 20 maggio 1970) per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati. Gli impianti di videosorveglianza non potranno essere utilizzati per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati o per finalità di promozione turistica.
Le immagini non potranno essere utilizzate per l'irrogazione di sanzioni per infrazioni al Codice della Strada, ma esclusivamente per l'eventuale invio da parte delle Centrali Operative di personale con qualifica di organo di polizia stradale per le contestazioni ai sensi del Codice della Strada.

CAPO II
OBBLIGHI PER IL TITOLARE DEL TRATTAMENTO

Art. 5 – Notificazione

Il Comune di ---, nella sua qualità di titolare del trattamento dei dati personali, rientrante nel campo di applicazione del presente regolamento, adempie agli obblighi di notificazione preventiva al Garante per la protezione dei dati personali, qualora ne ricorrano i presupposti, ai sensi e per gli effetti degli artt. 37 e 38 del Codice in materia di protezione dei dati personali approvato con decreto legislativo 30/6/2003, n. 196.

Art. 6 – Responsabile

1. Il Comandante della Polizia Municipale in servizio, o altra persona nominata dal Sindaco, domiciliati in ragione delle funzioni svolte in ----- presso il Comando della Polizia Municipale, è individuato, previa nomina da effettuare con apposito decreto del Sindaco, quale responsabile del trattamento dei dati personali rilevati, ai sensi per gli effetti dell'art. 2, lett. e). E' consentito il ricorso alla delega scritta di funzioni da parte del designato, previa approvazione del Sindaco.

2. Il responsabile deve rispettare pienamente quanto previsto, in tema di trattamento dei dati personali, dalle leggi vigenti, ivi incluso il profilo della sicurezza e dalle disposizioni del presente regolamento.

3. Il responsabile procede al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 1 e delle proprie istruzioni.

4. I compiti affidati al responsabile devono essere analiticamente specificati per iscritto, in sede di designazione.

5. Gli incaricati del materiale trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del titolare o del responsabile.

6. Il responsabile custodisce le chiavi per l'accesso ai locali della centrale di controllo, le chiavi degli armadi per la conservazione delle videocassette/cd o altro supporto informatico, nonché le parole chiave per l'utilizzo dei sistemi.

Art. 7 - Persone autorizzate ad accedere alla sala di controllo

1. L'accesso alla sala di controllo è consentito solamente, oltre al Sindaco o suo delegato, al personale in servizio del Corpo di Polizia Municipale autorizzato dal Comandante e agli incaricati addetti ai servizi, di cui ai successivi articoli.

2. Eventuali accessi di persone diverse da quelli innanzi indicate devono essere autorizzati, per iscritto, dal Comandante del Corpo di Polizia Municipale.

3. Possono essere autorizzati all'accesso alla centrale operativa solo incaricati di servizi rientranti nei compiti istituzionali dell'ente di appartenenza e per scopi connessi alle finalità di cui al presente regolamento, nonché il personale addetto alla manutenzione degli impianti ed alla pulizia dei locali, i cui nominativi dovranno essere comunicati per iscritto al Comandante del Corpo di Polizia Municipale.

4. Il Responsabile della gestione e del trattamento impartisce idonee istruzioni atte ad evitare assunzioni o rilevamento di dati da parte delle persone autorizzate all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali.

5. Gli incaricati dei servizi di cui al presente regolamento vigilano sul puntuale rispetto delle istruzioni e sulla corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.

Art. 8 - Nomina degli incaricati e dei preposti alla gestione dell'impianto di videosorveglianza

1. Il responsabile, designa e nomina i preposti in numero sufficiente a garantire la gestione del servizio di videosorveglianza nell'ambito degli operatori di Polizia Municipale.

2. I preposti andranno nominati tra gli Ufficiale ed Agenti in servizio presso la Centrale Operativa e nei vari settori operativi del Corpo di Polizia Municipale che per esperienza, capacità ed affidabilità forniscono idonea garanzia nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.

3. La gestione dell'impianto di videosorveglianza è riservata agli organi di Polizia Municipale, aventi qualifica di Ufficiali ed Agenti di Polizia Giudiziaria ai sensi dell'art. 55 del Codice di Procedura Penale.

4. Con l'atto di nomina, ai singoli preposti saranno affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi.

5. In ogni caso, prima dell'utilizzo degli impianti, essi saranno istruiti al corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente regolamento.

6. Nell'ambito degli incaricati, verranno designati, con l'atto di nomina, i soggetti cui è affidata la custodia e conservazione delle password e delle chiavi di accesso alla sala operativa ed alle postazioni per l'estrapolazione delle immagini.

Art. 9 - Accesso ai sistemi e parole chiave

1. L'accesso ai sistemi è esclusivamente consentito al responsabile, ai preposti come indicato nei punti precedenti.

2. Gli incaricati ed i preposti saranno dotati di propria password di accesso al sistema.

3. Il sistema dovrà essere fornito di "log" di accesso, che saranno conservati per la durata di anni uno.

CAPO III
TRATTAMENTO DEI DATI PERSONALI

Sezione I
RACCOLTA E REQUISITI DEI DATI PERSONALI

Art. 10 - Modalità di raccolta e requisiti dei dati personali

1. I dati personali oggetto di trattamento sono:
a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per le finalità di cui al precedente art. 4 e resi utilizzabili in altre operazioni del trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi, esatti e, se necessario, aggiornati;
c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
d) conservati per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto, per le quali essi sono stati raccolti o successivamente trattati ed in ogni caso pari al periodo di tempo stabilito dal successivo comma 3;

e) trattati, con riferimento alla finalità dell'analisi dei flussi del traffico, di cui al precedente art.4, comma 3, lett. d), con modalità volta a salvaguardare l'anonimato ed in ogni caso successivamente alla fase della raccolta, atteso che le immagini registrate possono contenere dati di carattere personale.

2. I dati personali sono ripresi attraverso le telecamere dell'impianto di videosorveglianza installate sul territorio comunale.

3. Le telecamere di cui al precedente comma 2 consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario. Il titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto attivato. I segnali video delle unità di ripresa saranno inviati presso la Centrale Operativa del Comando di Polizia Municipale. In questa sede le immagini saranno visualizzate su monitor e registrate su appositi server. L'impiego del sistema di videoregistrazione è necessario per ricostruire l'evento, per le finalità previste dal presente Regolamento. Le immagini videoregistrate sono conservate per un tempo non superiore a 72 (settantadue) ore successive alla rilevazione, presso la Centrale Operativa anche in caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. In relazione alle capacità di immagazzinamento delle immagini sui server, le immagini riprese in tempo reale sovrascrivono quelle registrate.

Art. 11 - Obblighi degli operatori

1. L'utilizzo del brandeggio da parte degli operatori e degli incaricati al trattamento dovrà essere conforme ai limiti indicati nel presente regolamento.

2. L'utilizzo delle telecamere è consentito solo per il controllo di quanto si svolga nei luoghi pubblici mentre esso non è ammesso nelle proprietà private.

3. Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo ammesso per la conservazione di cui al precedente articolo, solo in caso di effettiva necessità per il conseguimento delle finalità di cui all'art. 4 comma 3 e a seguito di regolare autorizzazione di volta in volta richiesta al Sindaco.

4. La mancata osservanza degli obblighi previsti al presente articolo comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla normativa vigente, di sanzioni amministrative oltre che l'avvio degli eventuali procedimenti penali.

Art. 12 - Informazioni rese al momento della raccolta

1. Il Comune di ----, in ottemperanza a quanto disposto dall'art. 13 del decreto legislativo 30/6/2003 n. 196, si obbliga ad affiggere un'adeguata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere su cui è riportata la seguente dicitura: " Polizia Municipale – Comune di ---- - Area videosorvegliata - Immagini custodite presso la Polizia Municipale di ----".

2. Il Comune di ---, nella persona del responsabile, si obbliga a comunicare alla comunità cittadina l'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, l'eventuale incremento dimensionale dell'impianto e l'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, ai sensi del successivo art. 15, con un anticipo di giorni dieci, mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale.

.

Sezione II
DIRITTI DELL'INTERESSATO NEL TRATTAMENTO DEI DATI

Art. 13 - Diritti dell'interessato

1. In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, ha diritto:
a) di ottenere la conferma dell'esistenza di trattamenti di dati che possono riguardarlo;
b) di essere informato sugli estremi identificativi del titolare e del responsabile oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati;
c) di ottenere, a cura del responsabile, senza ritardo e comunque non oltre 15 giorni dalla data di ricezione della richiesta, ovvero di 30 giorni previa comunicazione all'interessato se le operazioni necessarie per un integrale riscontro sono di particolare complessità o se ricorre altro giustificato motivo:
2. la conferma dell'esistenza o meno di dati personali che lo riguardano anche se non ancora registrati e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa

il trattamento; la richiesta non può essere inoltrata dallo stesso soggetto se non trascorsi almeno novanta giorni dalla precedente istanza, fatta salva l'esistenza di giustificati motivi.
3. la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati.
4. di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

5. Per ciascuna delle richieste di cui al comma 1, lett. c), n. 1), può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati e comprensivi dei costi del personale, secondo le modalità previste dalla normativa vigente.

6. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

7. Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.

8. Le istanze di cui al presente articolo possono essere trasmesse al titolare o al responsabile anche mediante lettera raccomandata, telefax o posta elettronica o comunicata oralmente, che dovrà provvedere in merito entro e non oltre quindici giorni.

9. Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Sezione III
SICUREZZA NEL TRATTAMENTO DEI DATI, LIMITI ALLA UTILIZZABILITA' DEI DATI E RISARCIMENTO DEI DANNI

Art. 14 - Sicurezza dei dati

1. I dati personali oggetto di trattamento sono custoditi ai sensi e per gli effetti del precedente art. 10, comma 3.

2. L'utilizzo dei videoregistratori impedisce di rimuovere il disco rigido su cui sono memorizzate le immagini.

Art. 15 - Cessazione del trattamento dei dati

1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati personali sono:
a) distrutti;
b) conservati per fini esclusivamente istituzionali dell'impianto attivato.

Art. 16 - Limiti alla utilizzabilità di dati personali

1. La materia è disciplinata dall'art. 14 del Codice in materia di protezione dei dati approvato con decreto legislativo 30 giugno 2003 n.196 e successive modificazioni e o integrazioni.
2.

Art. 17 - Danni cagionati per effetto del trattamento di dati personali

1. La materia è regolamentata per l'intero dall'art. 15 del Codice in materia di protezione dei dati approvato con decreto legislativo 30 giugno 2003 n.196 e successive modificazioni e o integrazioni.

Sezione IV
COMUNICAZIONE E DIFFUSIONE DEI DATI

Art. 18 – Comunicazione

1. La comunicazione dei dati personali da parte del Comune di Verona a favore di soggetti pubblici, esclusi gli enti pubblici economici, è ammessa quando è prevista da una norma di legge o regolamento.

In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria ed esclusivamente per lo svolgimento delle funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'art. 19 comma 2 del D.Lgs. 30/6/2003 n. 196.

2. Non si considera comunicazione, ai sensi e per gli effetti del precedente comma, la conoscenza dei dati personali da parte delle persone incaricate ed autorizzate per iscritto a compiere le operazioni del trattamento dal titolare o dal responsabile e che operano sotto la loro diretta autorità.

3. E' in ogni caso fatta salva la comunicazione o diffusione di dati richiesti, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'art. 58, comma 2, del D.Lgs. 30/6/2003 n. 196 per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

CAPO IV
TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Art. 19 – Tutela

1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli artt. 100 e seguenti del decreto legislativo 30 giugno 2003 n.196.

2. In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 4-6 della legge 7 agosto 1990, n. 241, è il responsabile del trattamento dei dati personali, così come individuato dal precedente art. 6.

CAPO V
MODIFICHE

Art. 20 - Modifiche regolamentari

1. I contenuti del presente regolamento dovranno essere aggiornati nei casi di aggiornamento normativo in materia di trattamento dei dati personali. Gli eventuali atti normativi, atti amministrativi dell'Autorità di tutela della privacy o atti regolamentari generali del Consiglio comunale dovranno essere immediatamente recepiti.

2. Il presente regolamento è trasmesso al Garante per la protezione dei dati personali a Roma, sia a seguito della sua approvazione, sia a seguito dell'approvazione di suoi successivi ed eventuali aggiornamenti.

Allegato:
UBICAZIONE TELECAMERE NEL COMUNE DI …..
2) PIAZZA
3) PIAZZA LATO ….
4) PIAZZA LATO ……

Carta per un utilizzo democratico della videosorveglianza

European Forum *for* Urban Security

>>> Preambolo

I sistemi di videosorveglianza conoscono, a seconda delle città europee, evoluzioni di diversa portata e natura, dovute tanto ai contesti nazionali e locali, quanto a considerazioni politiche, economiche, culturali e sociali.

Il presente progetto, che ha riunito dieci città, Genoa, Rotterdam, Liège, Le Havre, Ibiza, Saint-Herblain, Regione Veneto, Regione Emilia-Romagna, London metropolitan Police, Sussex Police, e un certo numero di esperti europei, si è proposto di ribadire, malgrado tali differenze, gli innegabili punti di convergenza, che costituiscono la base del nostro lavoro e attorno ai quali si articolano tecniche e strategie in materia di videosorveglianza.

Il primo punto di convergenza è costituito dalla necessità, nell'elaborazione e nel funzionamento dei dispositivi di videosorveglianza, di garantire il rispetto della vita privata dei cittadini e delle libertà fondamentali. L'articolo 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà individuali stabilisce al riguardo che.

« Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza.
Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto, a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui. »

L'obiettivo della presente Carta è quello di offrire ai cittadini le garanzie di cui hanno bisogno circa l'utilizzo di tali sistemi, poiché la videosorveglianza:

- può condizionare o alterare l'esercizio delle libertà individuali negli spazi pubblici dove viene effettuata;

- in considerazione delle evoluzioni tecnologiche che la caratterizzano, può spalancare innumerevoli possibilità, che aumenteranno in modo esponenziale;

- è una questione al centro di dibattiti appassionati che fanno emergere preoccupazioni e timori;

Ricollocare il cittadino al centro delle preoccupazioni delle città a proposito dei sistemi di videosorveglianza è stata la linea guda di questo progetto « Cittadini, Città e Videosorveglianza ». A tale finalità si aggiunge quella del rispetto e dell'applicazione del diritto all'intimità nello spazio pubblico, obiettivi verso i quali dobbiamo tendere.

Il secondo punto di convergenza è costituito dall'esigenza di mettere in pratica tale impegno, definendo dei modi di intervento che consentano di dargli concretezza e sostanza.

La Carta per un utilizzo democratico della videosorveglianza permette di conciliare questi due punti. Rappresenta, attraverso una serie di norme, l'impegno dei suoi firmatari. Enuncia principi fondatori ed elenca misure concrete e pragmatiche per l'attuazione di tali principi, il cui abbinamento ne fa uno strumento di supporto agli interventi.

Alcune raccomandazioni trasversali non si limitano tuttavia a invitare all'attuazione di un principio, per quanto unificatore. I partner del progetto hanno tenuto a evidenziarle, in quanto strumenti metodologici. Sono le quattro raccomandazioni seguenti:

- La realizzazione di una diagnosi preliminare, volta a definire in modo obiettivo i fabbisogni locali. Tale diagnosi deve inoltre permettere di valutare la fattibilità di un progetto di videosorveglianza su un determinato territorio. Deve essere per quanto possibile realizzata da un organismo esterno;

- La realizzazione di valutazioni periodiche, che servano in quanto strumento di supporto alle decisioni e permettano di rafforzare o di modificare il posizionamento di un sistema di videosorveglianza;

- La formazione degli operatori. Gli operatori della videosorveglianza sono la chiave di volta di tutto il sistema, il cui buon funzionamento dipende in parte da loro. Tali operatori devono essere adeguatamente formati circa i principi su cui poggia la presente carta, ma anche circa le raccomandazioni da mettere in opera. Devono altresì avere integrato e compreso gli obiettivi del sistema. La formazione è un'esigenza di qualità;

- Un'autorità di controllo deve permettere di verificare il rispetto dei principi della carta. L'istituzione di tale struttura locale può essere prevista dalla legislazione nazionale o rientrare nell'ambito di un approccio volontaristico delle città. L'indipendenza di tale autorità deve essere garantita nel miglior modo possibile.

>>> Il campo di applicazione della carta

La Carta disciplina l'elaborazione, il funzionamento e lo sviluppo di sistemi di videosorveglianza pubblici, vale a dire di quelli gestiti dalle autorità pubbliche, siano esse statali, regionali, provinciali o locali. Le norme che enuncia devono tuttavia potere essere applicate anche a sistemi di videosorveglianza privati, in particolare quando l'esercizio di tali impianti può essere devoluto alle autorità pubbliche.

I principi fondatori

Sono stati definiti sette grandi principi. Sono complementari e non devono essere compresi unicamente in relazione gli uni agli altri. Insieme, si rafforzano vicendevolmente, garantendo la loro perennità.

I. Il principio di liceità

I sistemi di videosorveglianza possono essere elaborati e sviluppati unicamente nel rispetto della legge e delle norme vigenti

Rispetto e conformità alle normative europee, nazionali, regionali o locali. Lo sviluppo di tali sistemi deve ugualmente essere realizzato nel rispetto delle norme in materia di tutela dei dati, dei testi in materia di intercettazioni di comunicazioni e di conversazioni, di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi per i quali esiste un'analoga protezione. Devono altresì essere prese in considerazione le norme relative alla tutela dei lavoratori.

RACCOMANDAZIONI E MODI DI AZIONE

I sistemi di videosorveglianza devono essere elaborati in coerenza con:

1) Il diritto europeo e internazionale:

- la Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) del Consiglio d'Europa – 1950;
- la Convenzione 108 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale– 1981;
- la Carta dei diritti fondamentali dell'Unione europea;
- la direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali; nonché alla libera circolazione di tali dati.

2) Le normative nazionali e locali che disciplinano i sistemi di videosorveglianza e il trattamento e la tutela dei dati personali;

-Valutare la pertinenza di un impianto di videosorveglianza rispetto agli obiettivi per i quali la Costituzione consente una limitazione all'esercizio dei diritti fondamentali dei cittadini

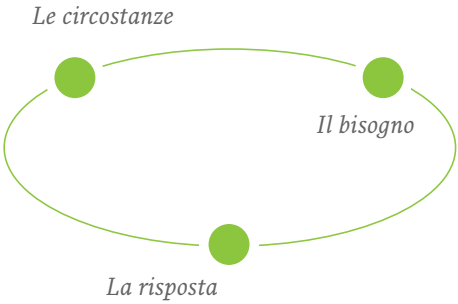
3) Le diverse giurisprudenze esistenti in materia;

4) In considerazione delle evoluzioni tecnologiche, in presenza di un vuoto normativo su una determinata questione, la realizzazione del sistema di videosorveglianza deve avvenire accertandosi che siano osservati gli altri principi definiti nella presente carta.

II. Il principio di necessità

L'impianto di un sistema di videosorveglianza non può costituire di per sé un'esigenza.

Deve essere deciso in base alle necessità. La necessità fa riferimento all'incontro tra determinate circostanze e un bisogno, da un lato, e la risposta fornita dal sistema di videosorveglianza, dall'altro lato. Tale bisogno e tali circostanze rendono pertinente la decisione, per cui l'azione diventa inevitabile. È il principio di necessità che sottende la decisione di installare un sistema di videosorveglianza. La necessità assume in tal modo una dimensione prescrittiva: « La necessità non conosce legge ».



L'incontro tra le circostanze e il bisogno è alla base della necessità della risposta.

A- LE CIRCOSTANZE

• Individuare in modo preciso, tramite un audit o una diagnosi, le problematiche di sicurezza e di prevenzione della delinquenza riscontrate sul territorio della città;

• Tracciare un bilancio delle risorse locali disponibili e dei dispositivi esistenti, che consentano di trovare risposte alla situazione diagnosticata;

B- IL BISOGNO

• Reperire i bisogni individuati nel corso della diagnosi e dell'inventario delle potenzialità locali. I bisogni devono essere precisati per quanto possibile, poiché da loro dipendono i futuri obiettivi del progetto;

• Considerare se altri mezzi meno intrusivi sono possibili per trovare risposte adeguate a queste problematiche;

C- LA RISPOSTA

• Occorre definire gli obiettivi e individuare i vantaggi e i risultati attesi dal sistema. Tali obiettivi devono essere tradotti in modi di funzionamento. Per esempio, bisognerà quindi definire quali sono gli aspetti e le implicazioni funzionali di un sistema di videosorveglianza finalizzato alla prevenzione della delinquenza;

• Stabilire il tipo di sistema che può consentire alla città di conseguire tali obiettivi in modo realistico; il sistema di videosorveglianza deve essere calibrato per rispondere in modo pertinente ed efficace ai fabbisogni individuati;

• Gli impianti di videosorveglianza possono essere attivati unicamente quando altre misure meno intrusive si sono rivelate insufficienti o inapplicabili (dopo una valutazione), o quando la natura del problema da risolvere non rientra nel campo di applicazione di tali altre misure. In ogni modo, la videosorveglianza deve rappresentare unicamente una parte di una risposta coordinata a un problema individuato;

• Autorizzarsi ad applicare il diritto di ritornare sulla decisione, ove necessario. Le città devono avere la possibilità di giudicare, sulla base di una valutazione, che la videosorveglianza non rappresenta più una necessità o che occorrerebbe una ridistribuzione delle telecamere;

III. Il principio di proporzionalità

L'elaborazione, l'installazione, il funzionamento e lo sviluppo dei sistemi di videosorveglianza devono rispettare la giusta misura.

Il dispiegamento dei sistemi di videosorveglianza deve essere commisurato ai problemi che intende risolvere. Tale ricerca di proporzionalità è anzitutto una questione di equilibrio tra gli obiettivi perseguiti e i mezzi messi in opera per conseguirli. Il principio di proporzionalità è pertanto intimamente legato alla nozione di equilibrio, che impone che l'impianto di videosorveglianza non costituisca l'unica risposta elaborata in una città in materia di sicurezza e di prevenzione della delinquenza.

RACCOMANDAZIONI / MODI DI AZIONE

La proporzionalità deve essere valutata a ogni fase e in ogni modalità del trattamento dei dati, in particolare allorquando occorre definire:

- La dimensione dell'impianto e le capacità tecniche delle telecamere
  - L'organizzazione tecnica e umana deve essere adattata allo stretto necessario, il che impone di utilizzare una tecnologia in grado di rispondere agli obiettivi assegnati, senza andare oltre. L'utilizzo di un sistema di videosorveglianza deve essere limitato nel tempo e nello spazio: a un momento determinato e su un territorio specifico, in risposta a un bisogno definito. Assegnare una nuova funzione al sistema di videosorveglianza richiede una riflessione sulla necessità (principio I).
  - Tale impianto tecnico dovrebbe integrare in particolare un sistema di occultamento delle aree private, mediante un mascheramento dinamico, poiché la videosorveglianza di spazi pubblici non può avere come « effetto secondario » la sorveglianza di uno spazio privato. È un imperativo da prendere in considerazione ugualmente quando si deve pianificare il posizionamento e la configurazione delle telecamere e il loro tipo (fissa o mobile);

● La tutela dei dati
Le immagini catturate dalle telecamere di videosorveglianza costituiscono dei dati personali e come tali devono essere tutelate. Il che impone l'osservanza di regole severe, relative alla registrazione, la conservazione, la condivisione e l'eventuale cancellazione o soppressione delle immagini. Occorre accertarsi del rispetto di tali norme quando si prendono decisioni riguardanti:

- lo stoccaggio delle immagini;
- la durata di un'eventuale conservazione dei dati, che comunque deve essere sempre temporanea. La durata di conservazione deve essere limitata allo stretto necessario, deve essere fissata e definita mediante parametraggio nel sistema;
- la protezione fisica e tecnica dei dati personali E' pertanto necessario definire i protocolli di gestione delle autorizzazione di accesso e di trattamento delle immagini. Occorre integrare in tali protocolli l'approccio « *Privacy by design* » che presuppone che la tutela dei dati personali sia presa in considerazione a monte, fin dal momento della progettazione degli impianti di videosorveglianza.

● I sistemi di videosorveglianza devono trovare il loro equilibrio e la loro proporzione in una politica integrata di sicurezza e di prevenzione della delinquenza. Sono uno strumento di una politica di sicurezza globale e devono pertanto essere coerenti con le altre risposte messe in atto localmente.

IV – Il principio di trasparenza

Qualsiasi autorità incaricata dell'applicazione di un sistema di videosorveglianza deve condurre una politica chiara e leggibile per quanto concerne il funzionamento del proprio sistema

È trasparente tutto quanto si vede dall'esterno. Dal momento che la videosorveglianza può essere considerata una tecnologia restrittiva delle libertà, deve essere utilizzata in modo completamente trasparente ed essere corredata da incisive campagne di informazione del pubblico.

• L'autorità che prende l'iniziativa di installare telecamere di videosorveglianza deve informare chiaramente i cittadini:

- sul progetto che prevede l'installazione di un sistema di videosorveglianza;
- sugli obiettivi delle telecamere;
- sui mezzi stanziati per la messa in servizio del sistema;
- sulle aree videosorvegliate. Al riguardo, è necessario utilizzare una segnaletica visibile e riconoscibile mediante un pittogramma;
- sull'identità, la funzione e il nome delle persone a cui rivolgersi per qualsiasi richiesta di informazioni. L'insieme di tali informazioni deve figurare sui cartelli che segnalano le aree videosorvegliate;
- sulle misure specifiche di tutela delle immagini registrate. I dati ottenuti mediante un sistema di videosorveglianza devono essere protetti con un accesso ristretto mediante password. Devono essere utilizzati unicamente per le finalità previste, dalle persone autorizzate e devono essere conservati il tempo necessario. Qualsiasi utilizzo delle immagini registrate deve essere notificato in un registro regolarmente aggiornato a tale scopo;
- sulle autorità che possono essere i destinatari di tali immagini registrate;
- sui loro diritti relativi alle immagini che li riguardano. Si tratta in particolare dei seguenti diritti:
  - Diritto di accesso alle proprie immagini, nel rispetto del diritto dei terzi. Tale diritto potrà essere rifiutato nel caso di indagini giudiziarie, oppure nel caso di rischi legati alla sicurezza e alla difesa nazionale;
  - Diritto di verifica della cancellazione delle immagini che li riguardano, superato il periodo di conservazione delle immagini;

Tali informazioni devono essere comprensibili ed espresse in un linguaggio chiaro e intelligibile.

• L'autorità responsabile del sistema dovrà informare regolarmente i cittadini sui risultati e il conseguimento degli obiettivi, tramite i mezzi di comunicazione utilizzati solitamente. Il che implica una

formulazione chiara degli obiettivi a monte, fin dall'avvio del progetto e richiederebbe delle valutazioni del dispositivo basate su indicatori predefiniti;

• È fortemente sconsigliato ricorrere a finte telecamere, dal momento che tale falsa informazione può screditare il sistema e impegnare la responsabilità dei gestori;

V – Il principio di responsabilità

Il diritto di sorvegliare gli spazi pubblici è riservato ad autorità da definirsi in modo restrittivo. Sono responsabili dei sistemi installati a loro nome.

Le autorità incaricate dei sistemi di videosorveglianza sono i garanti di un loro utilizzo legale e rispettoso della vita privata e delle libertà fondamentali. La loro responsabilità potrà quindi essere impegnata in caso di inosservanza o di violazioni constatate. Le autorità amministrative dinanzi alle quali tale responsabilità potrà essere invocata devono essere individuate chiaramente. Le aziende private che possiedono e gestiscono sistemi di videosorveglianza che riprendono spazi pubblici devono osservare le stesse norme delle autorità pubbliche.

RACCOMANDAZIONI / MODI DI AZIONE

• Comunicare i nomi dei referenti responsabili. Ogni segnaletica indicante l'area videosorvegliata potrà in particolare comportare tali informazioni;

• Affermare l'obbligo di riservatezza dei gestori del sistema, nell'ambito della definizione di un regolamento interno, oppure di un codice deontologico destinato ai gestori del sistema. La loro responsabilità potrà essere impegnata in caso di inosservanza di tale obbligo;

• Ricorrere a misure di sicurezza che consentano di tutelare l'accesso alla sala controllo del sistema, ma anche di proteggere l'accesso alle immagini immagazzinate. Devono essere messe in opera misure tecniche di controllo di tali accessi;

• Divulgare le modalità per la consultazione delle autorità amministrative incaricate di sanzionare ogni abuso constatato;

• Mettere in opera un meccanismo appropriato per la divulgazione delle informazioni necessarie per la comprensione da parte del pubblico dell'utilizzo della videosorveglianza.

VI – Il principio di supervisione indipendente

Un processo di controllo indipendente deve mettere in opera un sistema di freni e contrappesi per vigilare sul funzionamento della videosorveglianza.

Qualsiasi controllo presuppone la definizione di norme. Tale principio di supervisione indipendente consente, tramite il rispetto di queste norme, di armonizzare le pratiche nel senso indicato dalla Carta. Il processo di controllo indipendente può assumere più forme e intervenire a vari momenti nello sviluppo dei sistemi. Il « controllore indipendente » può essere una personalità qualificata, oppure un organo specifico composto in particolare da cittadini.

RACCOMANDAZIONI / MODI DI AZIONE

• Si raccomanda che il compito di fornire, dopo lo studio delle pratiche, le autorizzazioni per l'installazione dei sistemi di videosorveglianza spetti a tale autorità indipendente;

• La suddetta autorità indipendente deve inoltre essere incaricata di vigilare affinché la messa in opera e l'utilizzo del sistema rispettino le regole e norme definite.

VII – Il principio del coinvolgimento dei cittadini

Occorre adoperarsi per favorire il coinvolgimento dei cittadini in ogni tappa della vita di un sistema di videosorveglianza.

Il principio del coinvolgimento dei cittadini consiste nel dare la parola ai cittadini, attraverso varie forme di consultazione, di partecipazione, di deliberazione e di codecisione. Ogni nuova installazione o estensione di un impianto di videosorveglianza dovrà sempre prevedere l'attiva partecipazione dei cittadini residenti sul territorio, per esempio attraverso gruppi di discussione. Buona parte del successo di un sistema di videosorveglianza dipende dall'adesione degli abitanti.

RACCOMANDAZIONI / MODI DI AZIONE

• Consultare i cittadini per l'individuazione dei bisogni, nell'ambito della diagnosi preliminare, per esempio attraverso la realizzazione di indagini di vittimizzazione;

• Favorire un coinvolgimento iniziale dei cittadini per quanto riguarda l'installazione di telecamere, allorquando risponde a un bisogno. Può assumere la forma di "marce esplorative", nel corso delle quali i partecipanti percorrono un settore considerato problematico;

• Ricercare l'accettazione dei progetti di sicurezza globale da parte dei cittadini, organizzando, per esempio, delle riunioni pubbliche informative, per potere ottenere la loro adesione ai progetti del comune;

• Favorire la partecipazione dei cittadini al controllo e alla valutazione del sistema, tramite questionari di soddisfazione;

•Prevedere un processo ben inquadrato e formalizzato, che offra ai cittadini la possibilità di visitare la sala di controllo e di gestione del sistema di videosorveglianza, anche in modo estemporaneo. Qualsiasi rifiuto deve essere motivato (per esempio, per ragioni di un'indagine giudiziaria in corso). Tale possibilità deve essere definita e gestita in modo da non mettere in discussione il diritto di terzi;

• Rafforzare l'impegno delle autorità locali ad attivare uno strumento in grado di consentire la partecipazione regolare dei cittadini. La creazione di una struttura locale incaricata di vigilare sul buon utilizzo del sistema dovrà comprendere un'attiva partecipazione dei cittadini alla vita e allo sviluppo del sistema.

>>> Prospettive

Le città firmatarie della presente Carta si impegnano ad adoperarsi per applicarne i principi e per divulgarla nel loro ambito locale e nazionale.

Si impegnano altresì a continuare a scambiarsi opinioni al fine di adattare questa carta, in particolare alle evoluzioni tecnologiche.

Auspicano l'istituzione di un label e di una certificazione europea.

Sostengono l'idea di un linguaggio comune per rivolgersi ai cittadini europei, che si traduca nella creazione di una segnaletica europea delle aree videosorvegliate.

ARGOMENTIANCI

LINEE GUIDA PER I COMUNI IN MATERIA DI VIDEOSORVEGLIANZA ALLA LUCE DEL PROVVEDIMENTO GARANTE PRIVACY 8 APRILE 2010

EDIZIONI anci ComuniCare

AREA INFRASTRUTTURE
SICUREZZA E ATTIVITÀ PRODUTTIVE

Collana Argomenti Anci
ISBN 978-88-96280-22-5

La pubblicazione è stata curata da

ANCI – Area Infrastrutture, Sicurezza e Attività Produttive
Responsabile **Antonio Ragonesi**

In collaborazione con

l'Autorità Garante per la protezione dei dati personali

ComuniCare Anci

Amministratore unico
Giuseppe Rinaldi

Direttore editoriale
Danilo Moriero

Curatore della collana
Giuseppe Maria Galeone

Progetto grafico ed impaginazione
Fabiana Ridolfi
Daniele Zampa

ComuniCare srl
Via dei Prefetti 46
00186 Roma
comunicareanci.it
comunicare@anci.it

Si ringraziano per la collaborazione:

Claudio Filippi – Vice Segretario Generale e Direttore
Dipartimento Libertà Pubbliche e Sanità – Autorità Garante per la protezione dei dati personali
Luigi Altamura – *Comandante della Polizia Municipale di Verona*
Elena Fiore – *Comandante della Polizia Municipale di Forlì*
Antonella Manzione – *Vice Comandante Vicario della Polizia Municipale di Firenze*
Elsa Boemi – *Comandante della Polizia Municipale di Piacenza*

Si ringrazia in modo particolare il Comune di Verona per aver condotto in qualità di Capofila, il confronto tra le Amministrazioni.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Linee Guida per i Comuni in materia di Videosorveglianza alla luce del Provvedimento Garante Privacy 8 aprile 2010

AREA INFRASTRUTTURE
SICUREZZA E ATTIVITÀ PRODUTTIVE

Il Garante per la protezione dei dati personali con il Provvedimento generale emanato lo scorso 8 aprile 2010 ha fornito nuove regole in materia di videosorveglianza, aggiornando le disposizioni del 2004, anche alla luce delle nuove competenze attribuite ai Sindaci in tema di sicurezza urbana e per le diverse evoluzioni tecnologiche intervenute negli ultimi anni.

Nel corso dei lavori che hanno portato alla redazione finale del testo del Provvedimento e del confronto di profilo istituzionale con l'Associazione, è stata più volte richiamata l'esigenza di una collaborazione per fornire ulteriori indicazioni utili agli Enti Locali ed ai Comuni in particolare.

Si tratta per un verso di esplicitare le novità introdotte e per l'altro di porre l'accento sulla sfera dell'autonomia regolamentare dei Comuni. Ciò sempre nell'interesse principe di fornire ai cittadini nuovi strumenti a tutela della legalità e della sicurezza nel rispetto dei principi della privacy.

Per questo è importante che nella videosorveglianza, accanto al rispetto della sfera privata e del corretto utilizzo dei dati personali, i Comuni si dotino di regole affinché il servizio sia sempre più accessibile, trasparente, ed individuando al proprio interno precise responsabilità di gestione.

Sono queste le motivazioni che ci hanno indotto ad un lavoro di collaborazione, per il quale si ringrazia l'Ufficio del Garante della Privacy, che spero possa essere apprezzato perché intende fornire chiarimenti e strumenti di lavoro per una corretta applicazione, per quanto di competenza dei Comuni, circa l'utilizzo della videosorveglianza, anche ai fini della sicurezza urbana.

Le "linee guida" sono state realizzate a costo zero per la pubblica amministrazione e per l'ANCI. Sono il frutto del lavoro di confronto tra pubbliche amministrazioni, del lavoro prestato a titolo gratuito dalle risorse professionali "interne" ai Comuni, e in quanto tali "collaboratori" dell'ANCI, ed è forse un piccolo esempio di come ogni giorno la Pubblica Amministrazione riesce a realizzare collaborazioni e prodotti di alto livello valorizzando le risorse professionali di cui dispone.

Flavio Zanonato

Sindaco di Padova e Vice Presidente ANCI

“La videosorveglianza è divenuta oggi uno strumento indispensabile, nelle città, nei Comuni piccoli e grandi, alla tutela della sicurezza pubblica e al contrasto della criminalità, divenendo ormai parte integrante dell’arredo urbano, come i lampioni, le panchine, i semafori”.

Vorrei partire da questa verissima affermazione contenuta nelle Linee guida di Anci, per esprimere il mio apprezzamento per questo documento che contiene preziose indicazioni per i Sindaci e le Amministrazioni comunali sul corretto utilizzo dei sistemi di videosorveglianza.

Con la diffusione di queste Linee Guida, elaborate sulla scia del Provvedimento generale del Garante per la protezione dei dati personali, Anci non si limita a offrire ai sindaci un utilissimo strumento di lavoro per interpretare nel modo più corretto le regole stabilite dalla Autorità. Fa molto di più: dà un contributo importante ad assicurare che il bisogno di sicurezza e di rispetto e tutela della legalità, che è alla base dell’uso e della diffusione delle videocamere, sia assicurato sempre nel più attento rispetto dei principi di protezione dati, aiutando così tutti gli operatori a trovare il corretto punto di equilibrio fra sicurezza e libertà: due beni entrambi tanto preziosi quanto irrinunciabili, che nella vita quotidiana delle nostre comunità trovano il loro punto massimo di concretezza.

Grazie a queste Linee Guida i sindaci e i comuni italiani potranno essere, anche nell’esercizio delle nuove importanti competenze in materia di sicurezza urbana, esempio di sensibilità e attenzione alle esigenze reali delle comunità, nel solco di una tradizione che ha accompagnato lo sviluppo delle autonomie locali in tutta la storia dell’Italia unita e che ha trovato il suo massimo sviluppo nel quadro della Costituzione repubblicana. Una tradizione che ha sempre visto i Comuni promotori di libertà e capaci di dare risposte concrete ai bisogni reali dei cittadini in un quadro di democrazia, di legalità.

Tra le numerose indicazioni degne di nota, vorrei sottolineare innanzitutto quella che consiglia ai comuni di dotarsi di un Regolamento con cui individuare le finalità e le modalità del trattamento dei dati correlato a sistemi di videoripresa. A tale scopo l’Anci ha predisposto anche un schema tipo di Regolamento che merita apprezzamento e che potrà facilitare molto l’attività delle amministrazioni locali.

Particolarmente importanti, anche sul piano pratico, sono le indicazioni sulla presentazione della richiesta di verifica preliminare al Garante. Si chiarisce infatti che la stessa va fatta solo ed esclusivamente quando l'impianto di videosorveglianza raccolga immagini associate a dati biometrici; quando permetta, mediante apposito software, il riconoscimento della persona tramite collegamento o incrocio o confronto delle immagini rilevate (es. morfologia del volto) con altri specifici dati personali, in particolare con dati biometrici; quando si operi sulla base del confronto della relativa immagine con una campionatura di soggetti precostituita; quando l'impianto non si limiti a riprendere e registrare le immagini, ma sia in grado di rilevare automaticamente comportamenti o eventi anomali, di segnalarli, ed eventualmente di registrarli (sistemi c.d. intelligenti).

Sicuramente utilissime infine per le amministrazioni locali le tabelle riguardo le possibili sanzioni penali e amministrative in cui potrebbero incorrere i comuni anche con riguardo alle prescrizioni del Garante.

Il Garante non può che apprezzare lo sforzo compiuto, al quale ha anche concorso assicurando la piena collaborazione del suo Ufficio.

Queste Linee Guida rappresentano dunque anche un importante esempio di collaborazione istituzionale tra l'Anci e l'Autorità che, già avviata con la sottoposizione preventiva dello schema del provvedimento generale dell'Autorità al Ministero dell'Interno e alla stessa Anci, al fine di acquisire le loro valutazioni per i profili di competenza, ha trovato ora con questo documento e con il comune impegno a diffonderne il contenuto, e soprattutto la cultura della sicurezza e della privacy che ne è alla base, il suo più pieno sviluppo.

Francesco Pizzetti

Presidente dell'Autorità garante
per la protezione dei dati personali

ARGOMENTI

SOMMARIO

PARTE 1
Premesse 12

PARTE 2
Finalità 16

PARTE 3
Il Regolamento per la gestione di un sistema di vds comunale 18

PARTE 4
L'esame preventivo del Garante 20

PARTE 5
Sistemi di vds dotati di audio 26

PARTE 6
Sicurezza urbana e tempi di conservazione immagini 28

PARTE 7
Gestione impianti vds comunali a bordo mezzi pubblici 31

PARTE 8
Collegamenti tra centrali forze di polizia e polizie locali 34

PARTE 9
Procedure accesso immagini 37

PARTE 10
Vds e abbandono rifiuti: novità 40

PARTE 11
Utilizzo vds per rivelazioni violazioni in materia Codice strada 42

PARTE 12
Sanzioni 45

PARTE 13
Prescrizioni per il titolare del trattamento dati: 6 e 12 mesi 51

PARTE 14
Quesiti più frequenti 53

APPENDICE 56

ARGOMENTIANCI

Premessa

1ª Parte

Il nuovo Provvedimento del Garante per la Privacy in materia di videosorveglianza emanato l'08 aprile 2010[1] fornisce le regole da seguire in materia, novellando interamente il Provvedimento del 2004[2] che viene così abrogato e sostituito.

L'ANCI, con il presente documento intende fornire alcune specifiche, alla luce delle numerose novità e delle richieste di molte Amministrazioni comunali riguardo l'installazione e la gestione dei sistemi di videosorveglianza, visti gli investimenti economici intrapresi nell'ultimo periodo, grazie a contributi statali e regionali. L'ANCI, peraltro, ha fornito un proprio contributo nella stesura del documento in argomento attraverso un confronto con gli Uffici del Garante, così come hanno fatto il Ministero dell'Interno e l'Unione Province Italiane, istituzioni che hanno preventivamente valutato, secondo le rispettive competenze il Provvedimento stesso, suggerendone modifiche e miglioramenti, d'intesa con i Funzionari del Garante, con un nuovo spirito di collaborazione e condivisione di regole. Lo scopo è inoltre quello di omogeneizzare le varie procedure adottate e adottande in materia nei singoli comuni.

L'ANCI intende poi evidenziare ai singoli comuni il nuovo e stretto rapporto che è scaturito dalle importanti novità legislative approvate negli ultimi due anni in materia di sicurezza[3] e lo specifico campo della videosorveglianza.

Da non dimenticare ancora che l'Ufficio del Garante riceve, sempre in numero maggiore, reclami, proteste, richieste di verifiche preliminari e di controlli, in modo particolare da cittadini che ritengono violata la privacy, proprio dai sistemi di videosorveglianza gestiti dagli enti locali. Le ispezioni disposte dall'Ufficio del Garante in materia di videosorveglianza e non solo verso le amministrazioni comunali, con l'attivazione del Nucleo Servizio Privacy della Guardia di Finan-

za, hanno fatto peraltro emergere una serie di violazioni, con conseguenti sanzioni penali ed amministrative.

In materia di uso dei sistemi di videosorveglianza – ricorda il Garante – vengono applicate le disposizioni generali in tema di protezione dei dati personali.

Con il presente documento, l'ANCI vuole perciò fornire precise indicazioni ai Sindaci e alle Amministrazioni comunali, partendo dai concetti indicati nel Provvedimento dell'8 aprile 2010, considerato che la videosorveglianza è divenuta oggi uno strumento indispensabile, nelle città, nei Comuni piccoli e grandi, alla tutela della sicurezza pubblica e al contrasto della criminalità, divenendo ormai parte integrante dell'arredo urbano, come i lampioni, le panchine, i semafori.

Dal punto di vista criminologico, peraltro, la videosorveglianza viene definita *"una misura di prevenzione situazionale e più in particolare come una tecnica di sorveglianza formale"* (Clarke, 1997).

La necessità di adottare un aggiornamento all'importante e storico Provvedimento in materia datato anno 2004, è nata dalle finalità che i vari sistemi di videosorveglianza perseguono, dai successi che si sono conseguiti nei vari campi di azione, dalla necessità di imprimere un maggior rispetto delle regole sia per chi progetta, costruisce e amministra i sistemi, sia per chi li utilizza come le Forze di Polizia dello Stato e le Polizie Locali, queste ultime oggi sempre più chiamate a contribuire alla salvaguardia dei propri cittadini, secondo le direttive dei Sindaci, che hanno visto aumentare i propri poteri in materia di sicurezza, anche a seguito dell'approvazione del c.d. "Pacchetto Sicurezza 2008" che ha introdotto importanti modifiche all'art. 54 del T.U.E.L. e all'emanazione di moltissime ordinanze sindacali a tutela della cd "sicurezza urbana".

L'introduzione, per la prima volta nella storia italiana, della dizione di "sicurezza urbana", come indicata dal Decreto Ministro Interno del 5 agosto 2008[4] e i conseguenti provvedimenti emessi a mezzo di specifiche ordinanze sindacali, dimostrano quali siano i maggiori compiti cui oggi i Sindaci sono chiamati in materia di pubblica incolumità, decoro, rispetto delle regole di convivenza sociale, sicurezza primaria e secondaria, in un quadro normativo peraltro rispettoso

dei ruoli delle Autorità Provinciali di Pubblica Sicurezza (Prefetto e Questore) ex legge nr. 121/1981.

Il Garante per la Protezione dei Dati Personali ha così tenuto conto, nel Provvedimento in argomento, dell'evoluzione normativa in materia di sicurezza, impressa dal Parlamento tra il 2008 e il 2009, con norme che vanno ad incidere sui diritti dei cittadini, i quali non devono subire incursioni nella loro vita privata e nelle attività quotidiane, oltre a considerare i più moderni sistemi tecnologici, che oggi risultano rintracciabili nella commercializzazione di impianti di videosorveglianza.

Va perciò sempre ricordato che la necessità di garantire livelli elevati di tutela dei diritti e delle libertà individuali fondamentali rispetto al trattamento dei dati personali, permette l'utilizzo di nuovi e innovativi sistemi di videosorveglianza. Le Amministrazioni comunali devono sapere che la scelta meno costosa, più rapida o di più semplice attuazione però non è sempre la scelta migliore, in termini di impatto sulla protezione dei dati personali.

[1] Documento web: http://www.garanteprivacy.it/garante/doc.jsp?ID=1712680 pubblicato nella Gazzetta Ufficiale del 29 aprile 2010
[2] Documento web: http://www.garanteprivacy.it/garante/doc.jsp?ID=1003482
[3] Cd "Pacchetto Sicurezza 2008" D.L. nr. 92/2008 convertito in Legge 24 luglio 2008 nr. 125 e cd "Pacchetto Sicurezza 2009" Legge 15 luglio 2009, nr. 94.
[4] Decreto Ministro Interno 5 agosto 2008, pubblicato in Gazzetta Ufficiale nr. 186 del 09 agosto 2008 (docuweb http://www.interno.it/mininterno/export/sites/default/it/sezioni/servizi/legislazione/sicurezza/0989_2008_08_05_decreto_poteri_sindaci.html)

ARGOMENTIANCI

Finalità

2ª PARTE

Il Garante per la Protezione dei Dati Personali nel Provvedimento in argomento ha individuato tra le finalità per l'utilizzo della videosorveglianza, **quattro ambiti generali** che riguardano anche le specifiche competenze dei Comuni attraverso i propri organi, tra cui la protezione e l'incolumità degli individui, ivi compresi i profili attinenti alla sicurezza urbana (di stretta competenza dei Sindaci), all'ordine e alla sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati svolti dai soggetti pubblici (tra cui rientra la Polizia Locale), alla razionalizzazione e miglioramento dei servizi al pubblico, volti anche ad accrescere la sicurezza degli utenti.

Altra finalità individuata dal Garante attiene **la protezione della proprietà**, in particolare sui Sindaci ricade la titolarità della gestione degli impianti di videosorveglianza posti a protezione di sedi, palazzi, uffici, biblioteche, musei, luoghi pubblici.

Ancora con riferimento alla **rilevazione, prevenzione e controllo delle infrazioni** svolti da soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge, vanno evidenziate le attribuzioni in materia di Codice della Strada, in cui le competenze delle Polizie Locali in qualità di organo di polizia stradale[5], sono previste nell'utilizzo di sistemi di videocontrollo, oggi ancora più ampliati dalla recente modifica dello stesso Codice con Legge nr. 120/2010 del 29 luglio u.s.[6]

L'ultimo ambito indicato dal Garante tra le principali finalità nell'utilizzo di un impianto di videosorveglianza, è quello **dell'acquisizione di prove**, e in tal senso occorre ricordare la competenza di polizia giudiziaria posseduta dagli agenti ed ufficiali della Polizia Locale, che dipendono dalla competente Autorità Giudiziaria, secondo l'art. 109 della Costituzione e le norme del Codice di Procedura Penale.[7]

[5] Art. 12 del Codice della Strada Decreto Legislativo 30 aprile 1992 nr. 285 e succ. modif. *"Espletamento dei servizi di polizia stradale (omissis) d bis) ai corpi e ai servizi di polizia provinciale, nell'ambito del territorio di competenza; e) ai Corpi e ai servizi di polizia municipale, nell'ambito del territorio di competenza;*

[6] Art. 201 c. 1 bis e ter del Codice della Strada, così modificato dall'art. 36 della Legge 120/2010

[7] Art. 57 Codice Procedura Penale DPR 22 settembre 1988, nr. 447 *"Ufficiali ed Agenti di Polizia Giudiziaria. Sono agenti di polizia giudiziaria:a) il personale della polizia di Stato al quale l'ordinamento dell'amministrazione della pubblica sicurezza riconosce tale qualità;b) i carabinieri, le guardie di finanza, gli agenti di custodia, le guardie forestali e, nell'ambito territoriale dell'ente di appartenenza, le guardie delle province e dei comuni quando sono in servizio".*

ARGOMENTIANCI

Il Regolamento per la gestione di un sistema di VDS comunale

3ª parte

Nel precedente Provvedimento datato 2004, era espressamente prevista la predisposizione dell'*"atto di documentazione delle scelte"*. Tale atto ora non è più previsto lasciando alla sfera dell'autonomia dell'Ente l'adozione degli strumenti regolatori.

Il Garante per la Protezione dei Dati Personali tuttavia mostra come necessari, la corretta individuazione di specifiche finalità e di tutta una serie di altre attività come ad esempio l'individuazione delle figure dei responsabili e degli incaricati del trattamento delle immagini, le modalità di accesso alle immagini, di conservazione dei datie molti altri aspetti, richiamati nel Provvedimento dell'8 aprile 2010.

L'ANCI sottolinea come sia non solo auspicabile ma necessaria l'adozione di un Regolamento, a sostegno degli atti deliberativi e delle determinazioni dell'Ente Locale, quale massimo strumento di legittimazione e condivisione, per un corretto utilizzo di applicazioni così invasive.

L'ANCI ricorda, inoltre, che il testo del Regolamento per la gestione di un impianto di videosorveglianza non deve essere trasmesso agli Uffici del Garante per l'approvazione e neppure per la doverosa conoscenza. Il Regolamento dovrà essere però posto in visione durante le eventuali ispezioni dei Funzionari dell'Ufficio Ispettivo del Garante.

L'ANCI rammenta poi, come la predisposizione del Regolamento sia una forma di grande trasparenza amministrativa nei confronti dei cittadini, che vedrebbero così protetti i propri dati personali, secondo regole chiare, inderogabili e incisive.

A tale scopo è stato predisposto un testo di Regolamento Comunale per la gestione di un sistema di videosorveglianza da considerarsi indicativo, contenente gli aspetti di fondamentale importanza.

ARGOMENTIANCI

L'esame preventivo del Garante

4ª PARTE

Il Garante, dopo l'adozione del Provvedimento in materia di videosorveglianza dell'8 aprile 2010[8], ha riscontrato l'invio di copiosa corrispondenza da parte di diversi enti locali che hanno erroneamente ritenuto che fosse necessario sottoporre all'esame preventivo dell'Autorità l'installazione di qualsiasi impianto di videosorveglianza.
Al riguardo, l'ANCI ritiene opportuno fornire le seguenti precisazioni.

Quando non occorre l'esame preventivo del Garante

A| I normali sistemi di videosorveglianza

Il comune che intenda installare un sistema di videosorveglianza **non deve sottoporlo all'esame preventivo del Garante**; come stabilito con il provvedimento dell'8 aprile 2010, ma è sufficiente che il trattamento dei dati personali effettuato tramite tale tipo di impianto per lo svolgimento dei propri compiti istituzionali, avvenga previa **informativa** alle persone che stanno per accedere nell'area videosorvegliata, utilizzando a tale fine il modello semplificato predisposto in ***fac-simile*** dall'Autorità, e siano adottate **idonee misure di sicurezza**.

B| I sistemi integrati di videosorveglianza

L'utilizzo di **sistemi integrati di videosorveglianza**, ivi compresi quelli che consentono di rendere disponibili le immagini alle Forze di Polizia, **non deve essere sottoposto a verifica preliminare** nei casi in cui possano essere applicate, oltre alle generali misure di sicurezza (individuate dal Garante nel punto 3.3.1 del provvedimento dell'8 aprile 2010) le seguenti specifiche ulteriori misure che prevedono:

1. l'adozione di sistemi idonei alla **registrazione degli accessi** logici degli incaricati **e delle operazioni compiute sulle immagini registrate**, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei responsabili da parte del titolare, comunque non inferiore a sei mesi;

1. la **separazione** logica delle immagini registrate dai diversi titolari.

Ove siano rispettate tali specifiche prescrizioni di sicurezza, pertanto, **non occorre alcuna richiesta di verifica preliminare** per l'installazione di sistemi integrati di videosorveglianza che consentano:

a) *la* gestione coordinata di funzioni e servizi tramite **condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari** del trattamento, i quali utilizzano le medesime infrastrutture tecnologiche; in tale ipotesi, i singoli titolari possono trattare le immagini solo nei termini strettamente funzionali al perseguimento dei propri compiti istituzionali ed alle finalità chiaramente indicate nell'informativa, nel caso dei soggetti pubblici, ovvero alle sole finalità riportate nell'informativa, nel caso dei soggetti privati;

b) *il* collegamento telematico di diversi titolari del trattamento ad un **"centro" unico gestito da un soggetto terzo**; tale soggetto terzo, **designato responsabile** del trattamento ai sensi dell'art. 29 del Codice da parte di ogni singolo titolare, deve assumere un ruolo di coordinamento e gestione dell'attività di videosorveglianza senza consentire, tuttavia, forme di correlazione delle immagini raccolte per conto di ciascun titolare.

C| I sistemi integrati di videosorveglianza per la sicurezza urbana nei comuni

Con specifico riferimento all'attività del controllo sul territorio da parte dei comuni, anche relativamente a quanto disposto in materia di videosorveglianza comunale per finalità di **sicurezza urbana**, **non deve essere sottoposto a verifica preliminare** del Garante il trattamento dei dati effettuato tramite **sistemi integrati di videosorveglianza** qualora:

a) l'utilizzo condiviso, in forma integrale o parziale, di sistemi di videosorveglianza tramite la medesima infrastruttura tecnologica sia configurato con modalità tali da permettere ad **ogni singolo ente** e, in taluni casi, anche alle diverse strutture organizzative dell'en-

te, **l'accesso alle immagini** solo nei termini strettamente funzionali allo svolgimento dei **propri compiti istituzionali**, evitando di tracciare gli spostamenti degli interessati e di ricostruirne il percorso effettuato in aree che esulano dalla competenza territoriale dell'ente;

b) un **"centro" unico** gestisca l'attività di videosorveglianza per conto di diversi soggetti pubblici; in tale caso i dati personali raccolti dovranno essere **trattati in forma differenziata e rigorosamente distinta**, in relazione alle competenze istituzionali della singola pubblica amministrazione.

D| Durata della conservazione delle immagini

I comuni, per le attività di videosorveglianza finalizzata alla **sicurezza urbana**, possono conservare i dati registrati fino a "**sette giorni** successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione". Appare opportuno precisare che **non deve essere sottoposta ad una verifica preliminare** del Garante l'esigenza di conservare le immagini anche oltre il periodo di una settimana sopra indicato qualora intervenga una **specifica richiesta in tale senso dell'autorità giudiziaria o di polizia giudiziaria** in relazione a un'attività investigativa in corso.

Solo nel caso in cui il Comune intenda procedere, per speciali esigenze, a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una verifica preliminare del Garante.

E| Ulteriori casi di esclusione della verifica preliminare

Non si deve richiedere comunque una verifica preliminare purché siano rispettate tutte le seguenti condizioni:

a) il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti;

b) la fattispecie concreta, le finalità del trattamento, la tipologia e le modalità d'impiego del sistema che si intende adottare, nonché le categorie dei titolari, corrispondano a quelle del trattamento approvato;

c) si rispettino integralmente le misure e gli accorgimenti conosciuti o concretamente conoscibili prescritti nel provvedimento di cui alla lett. a) adottato dal Garante.

Quando occorre l'esame preventivo del Garante

Il comune **deve sottoporre all'esame preventivo del Garante** solo ed esclusivamente i trattamenti di dati che intende effettuare mediante un impianto di videosorveglianza che:

1. raccolga **immagini associate a dati biometrici**

2. permetta, mediante apposito *software*, il **riconoscimento della persona tramite collegamento** o incrocio o confronto delle immagini rilevate (es. morfologia del volto) con altri specifici dati personali, in particolare **con dati biometrici**, o sulla base del confronto della relativa immagine **con una campionatura di soggetti precostituita** alla rilevazione medesima oppure

3. non si limiti a riprendere e registrare le immagini, ma sia in grado di **rilevare automaticamente comportamenti o eventi anomali**, segnalarli, ed eventualmente registrarli (sistemi c.d. intelligenti).

Fuori dalle predette ipotesi, occorre richiedere una verifica preliminare nei soli casi in cui i trattamenti effettuati tramite videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti individuati dal Garante, sinteticamente sopra richiamati, non possano essere integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare.

Pagamento dei diritti di segreteria per richiesta esame preventivo

È qui il caso di ricordare che nella richiesta di esame preventivo agli uffici del Garante, i comuni dovranno versare all'Autorità i diritti di segreteria, il cui ammontare è stato quantificato, con determinazione del 15 gennaio 2005, nella misura di euro 1000,00 (mille).
Il versamento di tale importo può essere effettuato secondo una delle modalità di seguito indicate:

– mediante bonifico sul conto corrente bancario n. 18373 presso la Banca Popolare di Lodi, Agenzia n. 2 di Roma (ABI 05164; CAB 03202; CIN C);

– sul conto corrente postale n. 96677000, intestato a: "Garante per la protezione dei dati personali, Piazza di Monte Citorio, 121; 00186; Roma";

– con assegno circolare non trasferibile da intestare a "Garante per la protezione dei dati personali" e da inviare, al recapito già indicato, con posta assicurata.

[8] *Provvedimento in materia di dell'8 aprile 2010 (in Gazzetta Ufficiale n. 99 del 29 aprile 2010 e disponibile sul sito www videosorveglianza.garanteprivacy.it doc. web n. 1712680)*

ARGOMENTIANCI

Sistemi di VDS dotati di audio

5ª PARTE

L’ANCI sottolinea l’estrema delicatezza nell’utilizzo di impianti di videosorveglianza dotati di sistemi di registrazione audio, seppur commercializzati e proposti da aziende del settore. Tali tecnologie incidono in maniera importante nella privacy dell’individuo, configurando una interferenza illecita nella vita privata, fattispecie questa che prevede sanzioni penali. Solamente l’autorità giudiziaria può disporre registrazioni audio con tali sistemi, abbinati alle immagini di luoghi, locali, ambienti ben individuati.

ARGOMENTIANCI

Sicurezza Urbana e tempi di conservazione immagini

6ª PARTE

L'ANCI ricorda che l'art. 1 comma 1 della Legge 23 aprile 2009, nr. 38, che ha convertito in Legge con modificazioni il D.L. 23 febbraio 2009, nr. 11 ed ha previsto che "*per la tutela della sicurezza urbana, i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico",* oltre che *"la conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza e' limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione".*

È certamente una importante novità per gli Enti Locali, che prima utilizzavano in via limitata la videosorveglianza, visto che da una attenta lettura del Codice sulla Privacy (D.to L.vo nr. 196/2003)[9] e dalle conseguenti indicazioni del Garante, potevano sussistere limiti alle attività. In buona sostanza la legittimità delle riprese effettuate dalla Polizia Locale è sempre stata collegata alle finalità tradizionali dei Comuni ovvero il controllo del traffico, la prevenzione degli atti vandalici in determinate zone, il mantenimento della sicurezza nelle grandi città come nei piccoli comuni.

Occorre peraltro ricordare che le qualifiche possedute dagli appartenenti alla Polizia Locale riguardano la polizia stradale, la polizia amministrativa, la polizia giudiziaria e la sicurezza pubblica con finalità di ausilio alle Forze di Polizia ex Legge nr. 121/1981 (cfr. Legge Quadro sull'ordinamento della polizia municipale nr. 65/1986).

Per i comuni, l'aumento fino a sette giorni del tempo di conservazione delle immagini degli apparati di videosorveglianza utilizzati per finalità di sicurezza urbana, permette di accedere ad un consistente patrimonio di informazioni, che possono risultare utili per finalità di polizia giudiziaria e di pubblica sicurezza.

L'ANCI ricorda ancora che deve essere prestabilita la necessità di conservazione delle immagini stesse in luoghi (centrali operative, sale servizi) ove l'accesso sia limitato a persone individuate, mentre l'estrapolazione delle immagini deve avvenire per specifiche finalità. È stato specificato nuovamente che oltre il tempo previsto dalla norma della Legge nr. 38/2009, le immagini vanno cancellate anche con altre registrate in sovrascrittura. Occorre inoltre tener conto di un recente provvedimento del Garante per la Privacy[10] che ha riguardato un obiettivo sensibile

per finalità di terrorismo, nel quale il gestore del sistema di videosorveglianza ha ottenuto l'autorizzazione a conservare le immagini dei trenta giorni antecedenti. L'attuale norma che prevede una vera e propria clausola di salvaguardia (*"fatte salve speciali esigenze di ulteriore conservazione")* di cui alla legge 38/2009, va posta in equilibrio attraverso un percorso istituzionale e con interventi specifici per evitare abusi; la richiesta di allungamento dei tempi di conservazione dovrebbe essere preventivamente richiesta dal Comune al Comitato Provinciale per l'Ordine e la Sicurezza Pubblica, e sarà l'Ente Locale, titolare del trattamento, a richiedere la verifica preliminare al Garante per un eventuale allungamento del tempo di conservazione, per specifiche ed eccezionali finalità, nel rispetto del principio di proporzionalità.

[9] Decreto Legislativo 30 giugno 2003, nr. 196 http://www.garanteprivacy.it/garante/doc.jsp?ID=1311248
[10] http://www.garanteprivacy.it/garante/doc.jsp?ID=

ARGOMENTIANCI

Gestione impianti VDS comunali a bordo mezzi pubblici

7ª PARTE

Con riferimento al luogo in cui è attiva, vanno distinti vari aspetti della videosorveglianza, analizzando quella installata a bordo di autobus/tram/metropolitane urbani ed extraurbani, alle fermate del trasporto pubblico locale, a bordo di taxi, in stazioni, autostazioni, aeroporti. Già nel marzo 1999 il Garante rispondendo ad un quesito di un comune diede importanti prescrizioni, che vanno certamente confermate, condivise ed implementate.

I sistemi di videosorveglianza spesso sono gestiti dai Comuni e dalle Aziende Municipalizzate di Trasporto Pubblico, anche in base a specifici accordi e protocolli con le locali Prefetture e Questure; in alcuni casi questi sistemi sono collegati alle centrali operative delle Forze dell'Ordine che possono ricevere anche in diretta le immagini provenienti dai mezzi pubblici, in caso di allarme o di emergenza. Va perciò garantita la massima riservatezza, permettendo l'accesso sia in diretta che in remoto esclusivamente a personale qualificato e ben individuato, quali appartenenti alle Forze di Polizia dello Stato e delle Polizie Locali, sia a personale di aziende pubbliche e private con finalità di tutela del patrimonio dei mezzi pubblici.

L'ANCI ritiene di ricordare che le immagini a bordo dei mezzi di trasporto pubblico non possono essere viste dal personale appartenente ai servizi del trasporto pubblico e alla loro estrazione dovrà essere autorizzato personale in possesso di specifiche credenziali, che potrà accedere mediante sistemi "criptati", con utilizzo di *password* e *userid*; dovrà essere altresì garantita anche la registrazione dei *log* relativi alle attività di estrazione delle immagini, dove sono individuabili volti e particolari molto invasivi.

L'ANCI ricorda come sia importante prestare la massima attenzione nel rispetto e nella tutela dei lavoratori a bordo dei mezzi di trasporto pubblico videosorvegliati, affinchè lo strumento invasivo delle telecamere sia esclusivamente di prevenzione di atti criminosi e conseguente aumento della sicurezza del trasporto pubblico locale.

Per quanto attiene la videosorveglianza alle fermate del trasporto pubblico, l'ANCI fa presente che i sistemi di videosorveglianza sono spesso di proprietà di Comuni e di Aziende Municipalizzate, in base a specifici accordi con le locali Prefetture, soprattutto a seguito dei famosi attentati di Londra e Madrid del 2005, quando fu elevata l'attenzione per la tutela del trasporto pubblico. Anche in questo caso esistono collegamenti in diretta con le centrali operative delle

Forze di Polizia dello Stato e delle Polizie Locali, con sistemi di estrapolazione delle immagini gestiti direttamente dalle forze dell'ordine. La visione in diretta ove specificatamente regolata, potrà essere consentita anche al personale delle Aziende Municipalizzate al solo fine di verificare in tempo reale le condizioni di afflusso alle varie fermate e monitorare eventuali criticità che influiscano sui tempi di percorrenza, vietando altresì di utilizzare zoom e primi piani dei passeggeri.

ARGOMENTIANCI

Collegamenti tra centrali forze di polizia e polizie locali

8ª PARTE

Come si accennava nella parte iniziale di questo documento, per finalità di sicurezza urbana, deve essere consentito ai Comuni l'utilizzo di adeguati sistemi di videosorveglianza, le cui immagini devono essere conservate e visionate in locali protetti gestiti dalle Polizie Locali e la cui estrapolazione deve avvenire sotto il controllo di personale qualificato delle medesime forze dell'ordine; possono essere previsti collegamenti con le centrali operative delle Forze di Polizia dello Stato, anche con collegamenti in rete e via fibra ottica[11]. È importante tenere conto della Circolare del Capo della Polizia datata 08 febbraio 2005[12], diretta ai Prefetti e avente per argomento la definizione delle "linee guida" in materia di videosorveglianza che ha definito nuovi scenari e confortato gli orientamenti manifestati dalle amministrazioni comunali, salvaguardando le attività delle Polizie Locali. Ancora oggi la circolare cui sopra è un "indiscusso caposaldo del sistema, in particolare per ciò che attiene la sicurezza primaria e secondaria"[13].

È stato codificato nell'aggiornamento del Provvedimento in argomento che, salvo per gli obiettivi rilevanti per la c.d. sicurezza primaria e sia pure con ampie cautele, l'attività di gestione e di controllo degli apparati di videosorveglianza possa essere effettuata dalle Polizie Locali, a seconda degli obiettivi da vigilare, fatta salva la possibilità di prevedere, in condizioni contingenti, anche collegamenti diretti con le forze dell'ordine.

In un'ottica di collaborazione tra istituzioni in materia di sicurezza e di coinvolgimento delle autorità locali di pubblica sicurezza, l'ANCI ritiene che ogni nuova installazione dei sistemi di videosorveglianza da parte dei comuni debba passare l'esame preliminare del Comitato Provinciale per l'Ordine e la Sicurezza Pubblica.

I comuni, nella fase di progettazione ed installazione dei sistemi di videosorveglianza, dovranno però adottare tutte le cautele che vadano a prevenire eventuali forme di intrusione nella privacy dei cittadini, sensibilizzando i tecnici e i progettisti, oltre che i responsabili e gli incaricati del trattamento; importante punto di riferimento è il provvedimento del Garante datato 7 ottobre 2007[14], con il quale è stato specificato che il comune deve adottare ogni accorgimento volto ad evitare la ripresa di persone in abitazioni private, delimitando, quindi, la dislocazione, l'uso dello zoom e, in particolare, l'angolo visuale delle telecamere in modo da escludere ogni forma

di ripresa, anche quando non c'è registrazione, di spazi interni di abitazioni private, attraverso eventuali sistemi di settaggio e oscuramento automatico, non modificabili dall'operatore.

Particolare attenzione deve essere prestata dai comuni alla segnaletica e ai modelli di informativa che devono tassativamente indicare, oltre alle finalità di sicurezza urbana, quelle di controllo e di conservazione delle immagini di propria competenza. Fatta eccezione per la recente novità in materia di "sicurezza urbana" che riguarda i comuni.

A tal proposito, l'ANCI ricorda l'importante e recente circolare del Capo della Polizia datata 6 agosto 2010[15], diretta ai Prefetti, con la quale per la prima volta, l'Ufficio Coordinamento e Pianificazione delle Forze di Polizia indica chiaramente come "***l'utilizzazione di sistemi di videosorveglianza per i luoghi pubblici o aperti al pubblico, qualora si profilino aspetti di tutela dell'ordine e della sicurezza pubblica, oltre a quelli di sicurezza urbana, possa determinare l'attrazione di tali apparecchiature nell'ambito delle previsioni di cui al punto 3.1.1 del Provvedimento del Garante, con conseguente applicazione dell'art. 53 del Codice in materia di protezione dei dati personali e relativo affievolimento di alcuni principi di garanzia, quali in particolare, quello dell'informativa di cui all'art. 13 del cennato Codice".***

[11] Sono numerosi i "Patti per la sicurezza" firmati tra il Ministero dell'Interno e le Amministrazioni Comunali che prevedono l'installazioni di nuove telecamere da parte dei Comuni (cfr. Torino, Milano, Verona, Prato, Modena, ecc.)
[12] Circolare Ministero Interno – Dipartimento PS – nr. 558/A/421.2/70/456 datata 8 febbraio 2005 "Sistemi di videosorveglianza. Definizione di linee guida in materia" http://portale.anci.it/Contenuti/Allegati/Direttiva%202005.pdf<
[13] Tale definizione è stata inserita nella recente circolare del 6 agosto 2010, a cura dell'Ufficio Coordinamento e Pianificazione Forze di Polizia
[14] Garante per la Privacy: Provvedimento del 4 ottobre 2007:Newsletter: No a telecamere pubbliche che riprendano interni di abitazioni
[15] Circolare Ministero dell'Interno – Dipartimento Pubblica Sicurezza – Ufficio Coordinamento e Pianificazione Forze di Polizia nr. 558/A/421.2/70/195969 del 6 agosto 2010 http://portale.anci.it/Contenuti/Allegati/circolare%208%20agosto%202010.pdf

ARGOMENTIANCI

Procedure accesso immagini

9ª parte

Riguardo l'accesso alle immagini per la videosorveglianza con finalità di sicurezza urbana, il Garante ricorda che tale operazioni devono essere funzionali rispetto ai compiti affidati dalle leggi. L'ANCI ritiene inoltre necessario individuare precise finalità e procedure per tali attività. Le immagini perciò potranno essere visionate:

- sulla base di denunce di atti criminosi da parte dei cittadini, per il successivo inoltro delle eventuali fonti di prova all'autorità giudiziaria;

- sulla base di segnalazioni relative ad atti criminosi accertate direttamente dagli organi di polizia in servizio sul territorio cittadino;

- sulla base di atti criminosi che vengono rilevati direttamente dagli operatori di polizia nel visionare le immagini trasmesse in diretta dalle telecamere, nell'esercizio delle proprie funzioni.

- sulla base di richieste specifiche per indagini da parte dell'autorità giudiziaria

- sulla base di ogni altra richiesta di specifici organi/autorità che siano espressamente autorizzati, secondo specifiche norme di legge.

Le immagini devono essere custodite in maniera protetta, in server dedicati e non su reti informatiche accessibili da tutti i dipendenti del comune; il luogo ove è presente il server contenente le immagini, deve essere accessibile mediante porte allarmate, l'accesso deve avvenire con la digitazione di codici a chiave alfa-numerica e gli uffici devono essere allarmati, nel caso di chiusura durante alcune ore del giornata.

L'ANCI suggerisce ai comuni in cui i server siano custoditi presso la Centrale Operativa della Polizia Locale, che l'accesso alla stessa debba avvenire, ad esempio, attraverso un videocitofono con l'identificazione immediata del dipendente autorizzato e di conseguenza impedire l'in-

gresso di personale non autorizzato, secondo il provvedimento di individuazione degli incaricati al trattamento e ai preposti, redatto dal Responsabile del sistema di videosorveglianza.

Aspetto da non sottovalutare è anche l'estrapolazione delle immagini, di cui dovrà rimanere traccia informatica. Ogni accesso ai server deve avvenire attraverso un *log* di sistema, che identifichi chiaramente (mediante *password* e *userid*) il dipendente che ha svolto le singole attività, secondo quanto previsto dalla nomina individuale che autorizza il trattamento delle immagini, anche se non espressamente previsto da specifico provvedimento del Responsabile del sistema di videosorveglianza.

ARGOMENTIANCI

VDS E ABBANDONO RIFIUTI: NOVITÀ

10ª PARTE

Grazie ad uno specifico quesito rivolto da un comune al Garante, nel fornire nuove istruzioni sull'utilizzo della videosorveglianza in materia di rifiuti, l'Autorità ha profondamente modificato nel Provvedimento dell'8 aprile 2010, il capitolo relativo al contrasto all'abbandono di immondizia, fenomeno che crea degrado urbano, e di conseguenza insicurezza reale e percepita, su tutto il territorio nazionale, per il quale vengono richiesti dai cittadini sempre maggiori interventi da parte dei sindaci e delle Amministrazioni Comunali.

Nello specifico tema, l'utilizzo della videosorveglianza da parte delle Polizie Locali (in qualità di organo di polizia amministrativa) o di funzionari di aziende municipalizzate, in possesso di apposita qualifica, ottenuta al termine di corsi di formazione e con decreti da parte dei sindaci, per sanzionare coloro che lasciano rifiuti di ogni genere lungo i margini delle strade, fuori dai cassonetti o dalle apposite isole ecologiche, è stato espressamente previsto nel Provvedimento dell'8 aprile 2010 al punto 5.2., che permette il sanzionamento proprio grazie all'art. 13 della Legge 24 novembre 1981, nr. 689[16] e successive modifiche.

L'ANCI ricorda quanto indicato dal Garante, cioè che *"l'utilizzo della videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure.."*, ad esempio con la presenza costante di agenti della Polizia Locale, con la predisposizione di strutture fisiche che impediscano l'abbandono dei rifiuti. Le sanzioni possono riguarda le modalità, la tipologia e l'orario di deposito dei rifiuti.

[16] Art. 13 comma 1, Legge nr. 689/1981"Atti di accertamento – Gli organi addetti al controllo sull'osservanza delle disposizioni per la cui violazione è prevista la sanzione amministrativa del pagamento di una somma di denaro possono, per l'accertamento delle violazioni di rispettiva competenza assumere informazioni e procedere a ispezioni di cose e di luoghi diversi dalla privata dimora, a rilievi segnaletici, descrittivi e fotografici e ad ogni altra operazione tecnica.

ARGOMENTIANCI

Utilizzo vds per rilevazioni violazioni in materia Codice Strada

11ª PARTE

L'ANCI ha apprezzato lo sforzo dell'Ufficio del Garante nel delineare in maniera molto particolareggiate ogni aspetto inerente l'utilizzo di dispositivi per la rilevazione di violazioni al Codice della Strada mediante sistemi di videosorveglianza.

La raccolta dei dati deve essere sempre pertinente e mai eccedente la finalità cui è preposto il titolare, senza invadere la sfera privata degli automobilisti, delimitando gli angoli di ripresa.

In materia di controllo velocità dei veicoli vanno rammentate alcune disposizioni ministeriali:
a) modalità di ripresa: le norme attuali in materia di controlli sui limiti di velocità e sui sorpassi, secondo il Regolamento di esecuzione e attuazione del Codice della Strada, attraverso dispositivi elettronici hanno trovato una puntuale applicazione con la **Direttiva Ministero dell'Interno del 14/8/2009 prot. 300/A/10307/09/144/5/20/3** *"Direttiva per garantire un'azione coordinata di prevenzione e contrasto dell'eccesso di velocità sulle strade",* che ha definito molti aspetti relativi ai controlli e alla tutela della privacy; sono state peraltro abrogate molte circolari che davano indirizzi operativi agli organi d polizia stradale, tra cui la circ. nr. 300/A/1/54584/101/3/3/9 del 3 ottobre 2002.

Sistemi di rilevazione degli accessi dei veicoli ai centri storici e Zone a Traffico Limitato (ZTL)

Sono ormai decine nei comuni più grandi ed estesi, i sistemi di videosorveglianza che controllano gli accessi alle Zone a Traffico Limitato, le Aree pedonali Urbane e le corsie riservate ai mezzi pubblici.

In questo caso occorre tener conto che le attività sanzionatorie sono svolte dalle Polizie Locali, secondo le norme previste dall'art. 7 del D.Lg. 30 aprile 1992, nr. 285 ("Nuovo Codice della Strada"). Il D.P.R. 22 giugno 1999, nr. 250 definisce in maniera molto dettagliata tutte le modalità inerenti la gestione degli accessi ai centri storici mediante sistemi elettronici.

Un aspetto da non trascurare è quello della conservazione delle immagini scattate al momento della commessa violazione. Per la notifica del verbale sono necessari oggi 90/100 giorni,

poi occorre prevedere altri tempi di conservazione per l'eventuale ricorso, in teoria fino all'emissione della cartella esattoriale, nel caso in cui il contravventore non intenda pagare il verbale entro i termini previsti dal Codice. Tutte le immagini delle violazioni vanno custodite in appositi server, non connessi ad alcuna rete interna, accessibile solo al personale avente la qualifica di appartenente ad organo di polizia stradale (ufficiale o agente) o espressamente autorizzato con apposita nota riservata al personale di aziende esterne, che non svolgono funzioni di verbalizzazione.

In base alle direttive impartite dal Ministero della Funzione Pubblica e al fine di migliorare i servizi verso i cittadini e consentire un accesso agli atti tempestivo, sono molti i Comandi Polizia Locale che consentono di accedere alle immagini delle fotografie scattate in occasione delle violazioni al Codice della Strada (che – lo ricorda il Ministero dell'Interno Servizio Polizia Stradale - non saranno mai allegate al verbale ma che molto spesso i contravventori chiedono agli organi di polizia stradale, ai sensi della L. 241/1990 e successive modifiche), attraverso propri portali internet, direttamente a casa. Per l'accesso in sicurezza, l'utente deve però essere in possesso ad esempio di almeno tre chiavi univoche (la targa del veicolo, la data della violazione, il numero del verbale riportato dal documento notificato all'intestatario dell'autoveicolo).

ARGOMENTIANCI

SANZIONI

12ª PARTE

L'ANCI richiama l'attenzione di tutte le amministrazioni comunali riguardo le possibili sanzioni sia penali che amministrative, queste ultime particolarmente onerose, in cui potrebbero incappare i comuni, a seguito di visite ispettive dello specifico Nucleo Tutela Privacy del Garante per la Protezione dei Dati Personali o a seguito di segnalazioni dei cittadini, che ritengono lesa la propria riservatezza. Qui di seguito si indicano le principali sanzioni amministrative e penali:

PRINCIPALI SANZIONI AMMINISTRATIVE*

* Si osservano, in quanto applicabili, le disposizioni della Legge 24 novembre 1981, n. 689, e successive modifiche (art. 166, del Codice Privacy)

NORMA E TIPO D'INFRAZIONE	SANZIONE EDITTALE	PAGAMENTO IN MISURA RIDOTTA - DESTINAZIONE PROVENTI - AUTORITÀ COMPETENTE A RICEVERE IL RAPPORTO E AD IRROGARE LE SANZIONI	NOTE/OSSERVAZIONI
Omissione o inidoneità dell'informativa (es. laddove non è indicato il titolare del trattamento o la finalità perseguita) **Artt. 13 e 161 del Codice**	Sanzione amm.va da 6.000 € a 36.000 €	• 12.000 € entro 60 gg • Stato • Garante	v. punto 3.1 Provv. Garante dell'08/04/10 (Informativa)
Mancata o incompleta notificazione del trattamento dei dati personali al Garante **Artt. 37, 38 e 163 del Codice**	Sanzione amm.va da 20.000 € a 120.000 €	• 40.000 € entro 60 gg • Stato • Garante	v. punto 3.2 Provv. dell'08/04/10 (Prescrizioni specifiche). La violazione ricade su chiunque sia tenuto ad osservare tale prescrizione
Inosservanza dei provvedimenti di prescrizione di misure necessarie **Art. 162, comma 2-ter, del Codice**	Sanzione amm.va da 30.000 € a 180.000 €	• 60.000 € entro 60 gg • Stato • Garante	v. punto 3.3.1. nelle lettere da a) ad f) Provv. dell'08/04/10 (Misure di sicurezza)

NORMA E TIPO D'INFRAZIONE	SANZIONE EDITTALE	PAGAMENTO IN MISURA RIDOTTA - DESTINAZIONE PROVENTI - AUTORITÀ COMPETENTE A RICEVERE IL RAPPORTO E AD IRROGARE LE SANZIONI	NOTE/OSSERVAZIONI
Omessa adozione di misure minime di sicurezza **Artt. 33 e 162, comma 2-bis del Codice**	Sanzione amm.va da 10.000 € a 120.000 €	• Non è ammesso il p.m.r. • Stato • Garante	Tale violazione integra la fattispecie del reato ex art. 169 del Codice (Misure di sicurezza), che punisce con l'arresto fino a 2 anni, chi omette di adottare le prescritte misure di sicurezza. v. punto 3.3.2. Provv. dell'08/04/10 (Responsabili e incaricati)
Mancato rispetto dei tempi di conservazione delle immagini raccolte e collegato obbligo di cancellazione di delle immagini oltre il termine previsto **Art. 162, comma 2-ter, del Codice**	Sanzione amm.va Da 30.000 € a 180.000 €	• 60.000 € Entro 60 gg; • Stato • Garante	v. punto 3.4 Provv. dell'08/04/10
Omessa informazione o esibizione di documenti al garante Artt. 157 e 164, del Codice .	Sanzione amm.va 10.000 € a 60.000 €	• 20.000 € Entro 60 gg; • Stato • Garante	La violazione ricade su chiunque sia tenuto ad osservare tale prescrizione

Casi di minore gravità e ipotesi aggravate (art. 164-bis del Codice*)*

- Se taluna delle violazioni di cui agli artt. 161, 162, 163 e 164 è di minore gravità, avuto altresì riguardo alla natura anche economica o sociale dell'attività svolta, i limiti minimi e massimi stabiliti dai medesimi articoli sono applicati in misura pari a due quinti.
- In caso di più violazioni di un'unica o di più disposizioni in commento, a eccezione di quelle previste dagli artt. 162, comma 2, 162-bis e 164, commesse anche in tempi diversi in relazione a banche di dati di particolare rilevanza o dimensioni, si applica la sanzione amministrativa del pagamento di una somma da 150.000 € a 300.000 €. Non è ammesso il pagamento in misura ridotta.
- In altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati, i limiti minimo e massimo delle succitate sanzioni sono applicati in misura pari al doppio.
- Le sanzioni in oggetto possono essere aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore.

Pubblicazione del provvedimento del Garante (art. 165 del Codice)

Nei casi di cui ai suddetti articoli può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica. La pubblicazione ha luogo a cura e spese del contravventore.

Destinazione dei proventi (art. 166 del Codice)

I proventi, nella misura del 50% del totale annuo, sono riassegnati al fondo per le spese di funzionamento del Garante (*ex* art. 156, comma 10 del Codice), e sono utilizzati unicamente per l'esercizio dei compiti del suo Ufficio (artt. 154, comma 1, lett. *h)*, e 158 del Codice).

ILLECITI PENALI

IPOTESI DI REATO	SANZIONI PREVISTE	AUTORITÀ COMPETENTE	NOTE/OSSERVAZIONI
TRATTAMENTO ILLECITO DI DATI			
Trattamento illecito di dati personali da parte di soggetti pubblici (salvo che il fatto non costituisca più grave reato) Art. 167, comma 1 del Codice (1^ ipotesi)	Se ne deriva un danno: Reclusione da 6 mesi a 18 mesi; In caso comunicazione o diffusione dei dati: Reclusione da 6 mesi a 24 mesi	Procura della Repubblica presso il Tribunale Garante	Il fine è quello di trarre per sé o altri profitto o di recare ad altri un danno. Cfr. Artt. 18 e 19 del Codice
Trattamento illecito di dati personali da parte di soggetti pubblici (salvo che il fatto non costituisca più grave reato) Art. 167, comma 2 del Codice (2^ ipotesi)	Se ne deriva un danno: Reclusione da 1 a 3 anni	Procura della Repubblica presso il Tribunale Garante	Il fine è quello di trarre per sé o altri profitto o di recare ad altri un danno. Cfr. Artt. 17, 20, 21, 22 c.c. 8 e 11, e 45 del Codice
FALSITÀ NELLE DICHIARAZIONI O NOTIFICAZIONI			
Chiunque dichiari o attesti falsamente notizie o circostanze o produce atti o documenti falsi (salvo che il fatto costituisca più grave reato) Art. 168, comma 1 del Codice	Reclusione da 6 mesi a 3 anni	Procura della Repubblica presso il Tribunale Garante	Es. falsità nella notificazione del trattamento ex art. 37 del Codice, o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti

IPOTESI DI REATO	SANZIONI PREVISTE	AUTORITÀ COMPETENTE	NOTE/OSSERVAZIONI
		MISURE DI SICUREZZA	
Chiunque, essendovi tenuto, omette di adottare le misure minime di sicurezza. Art. 169, comma 1 del Codice	Arresto sino a 2 anni (reato contravvenzionale)	Procura della Repubblica presso il Tribunale Garante	v. Art. 33 del Codice Il c. 2 dell'art. 169 prevede una regolarizzazione entro un termine fissato dal Garante che estingue il reato (adempimento della prescrizione e pagamento di una sanzione amm.va. di 45.000 €, entro 6 mesi).
		INOSSERVANZA DI PROVVEDIMENTI DEL GARANTE	
Chiunque, essendovi tenuto, non osserva il provvedimento del Garante Art. 170, comma 1 del Codice	Reclusione da 3 mesi a 2 anni	Procura della Repubblica presso il Tribunale Garante	v. artt. 150 c.c. 1 e 2, e 143, c. 1 lett. c) del Codice
		PENE ACCESSORIE	

La condanna per uno dei delitti previsti dal D.Lgs. nr. 196 del 2003, prevede la pubblicazione della sentenza (art. 172 del Codice).

ARGOMENTIANCI

Prescrizioni per il titolare del trattamento dati: 6 e 12 mesi

13ª PARTE

L'ANCI ricorda alle Amministrazioni comunali che nella parte conclusiva del Provvedimento 8 aprile 2010, pubblicato nella Gazzetta Ufficiale del 29 aprile 2010 che ai sensi dell'art.154 comma 1, lett. c) del Codice della Privacy, viene prescritto al titolare del trattamento di dati personali effettuato tramite sistemi di videosorveglianza, di adottare al più presto e non oltre dei termini ben distinti di 6 o 12 mesi, decorrenti dal 29 aprile, le misure e gli accorgimenti illustrati nel documento.

TERMINE DATA	**MISURA – OBBLIGO**
ENTRO IL 29 OTTOBRE 2010	Sottoporre i trattamenti che presentano rischi specifici per i diritti e le libertà fondamentali degli interessati, alla verifica preliminare (art. 17 Codice Privacy – punto 3.2.1. Provvedimento)
ENTRO IL 29 OTTOBRE 2010	Adottare le misure necessarie per garantire il rispetto di quanto indicato nei punti 4.6 (Sistemi integrati di videosorveglianza: gestione coordinata di funzioni e servizi tramite condivisione delle immagini, collegamento ad un "centro" unico, adozione sistemi idonei alla registrazione accessi logici incaricati e delle operazioni compiute, separazione logica immagini registrate da diversi titolari) e 5.4 (avvertenze per i sistemi posti in essere da enti pubblici ed in particolare, da enti territoriali) per quanto concerne i sistemi integrati
ENTRO IL 29 APRILE 2011	Rendere l'informativa visibile anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno (non le finalità di "sicurezza urbana" come prima anticipato grazie alla circolare Ministero Interno 6 agosto 2010)
ENTRO IL 29 APRILE 2011	Adottare le misure di sicurezza a protezione dei dati registrati tramite impianti di videosorveglianza

ARGOMENTIANCI

Quesiti più frequenti

14ª PARTE

L'ANCI, per fornire un servizio innovativo e quanto più puntuale possibile, secondo quanto già indicato con alcuni pareri dal Garante per i Dati Personali alla luce del nuovo Provvedimento, intende dare risposta ad una serie di quesiti che riguardano moltissime Amministrazioni comunali, come da sotto indicato prospetto:

È necessario prevedere l'"atto di documentazione delle scelte" per l'installazione e la gestione di un sistema di videosorveglianza?
NO, non è più obbligatorio, ma l'ANCI consiglia i comuni di dotarsi di un Regolamento di Gestione della videosorveglianza, affinché l'Ente individui con atto determinato le finalità e le procedure del sistema stesso
Un comune ha installato un impianto di videosorveglianza per la duplice finalità di "sicurezza urbana" e "gestione del traffico". È necessaria la verifica preliminare?
E se l'impianto è collegato oltre che alla Polizia Locale, anche alle Forze di Polizia? NO, non è necessaria la verifica preliminare
Videosorveglianza e Zone a Traffico Limitato/Corsie Bus video sorvegliate: è necessario installare l'apposita informativa, individuato nell'allegato B del Provvedimento Garante 8 aprile 2010?
SI, và installato l'apposito segnale su specifica e autonoma struttura, affinché non sia visibile sul segnale stradale previsto dal Codice della Strada, ma per permettere al cittadino che accede ad una zona/area in cui sono in funzione collegate con Uffici in cu prestano servizi organi di polizia stradale
Le telecamere installate da un comune per finalità di "sicurezza urbana" e per la "sicurezza di edifici pubblici, sono dotate di funzione "motion detection". È necessaria la verifica preliminare?
SI
Alcune pattuglie della polizia locale di un comune sono dotate di telecamere per finalità di "sicurezza urbana", "sicurezza del personale che opera in aree a rischio" e "sanzionamento divieti di sosta – street control". Sussiste l'obbligo di informativa e se sì come , come si adempie all'obbligo di informativa?
SI, è sufficiente una indicazione segnaletica sul veicolo su cui è posizionata la telecamera mobile
I sistemi di videosorveglianza utilizzati per il sanzionamento degli accessi abusivi in ZTL o per il transito lungo le corsie riservate ai mezzi pubblici, che leggono le targhe dei veicoli, incrociandoli con data-base contenente le targhe autorizzate, necessitano di verifica preliminare?

NO, l'associazione delle immagini non avviene con dati biometrici o sensibili e pertanto creano pregiudizio agli interessati che vengono sanzionati

Un comune ha dato in gestione e manutenzione l'impianto di videosorveglianza a una ditta privata esterna all'amministrazione comunale. Quali adempimenti devono essere osservati?

La ditta deve essere nominata dal titolare dell'impianto, responsabile del trattamento e i suoi dipendenti abilitati a visionare le immagini devono ricevere una designazione ad hoc come incaricati

Un comune ha installato un impianto di videosorveglianza composto da una decina di telecamere e ha posizionato l'informativa indicata dal Provvedimento 8 aprile 2010, con cartelli solo all'ingresso del centro urbano. È sufficiente?

NO, perché dovrebbe essere collocato prima del raggio d'azione della telecamera e se il territorio è molto vasto non avrebbe più alcun senso. Differente è l'installazione di segnali per aree, perché più circoscritte rispetto all'intero territorio comunale

Un comune ha installato un sistema di videosorveglianza per finalità di "sicurezza urbana". È vero che sono affievolite alcune prerogative e alcuni obblighi?

SI, la circolare del Ministero dell'Interno del 6 agosto 2010 ha dichiarato che "…"

La Questura ha chiesto ad un comune di aumentare il tempo di conservazione delle immagini, oltre i 7 giorni. Quali attività deve svolgere il comune?

Il comune dovrà richiedere al Garante la "verifica preliminare", allegando la specifica richiesta della Questura e il parere del Comitato Provinciale per l'Ordine e la Sicurezza Pubblica. Occorrerà evidenziare se l'aumento del tempo di conservazione è a carattere permanente o provvisorio.

ARGOMENTIANCI

APPENDICE

SCHEMA DI NUOVO REGOLAMENTO PER LA DISCIPLINA DELLA VIDEOSORVEGLIANZA NEL TERRITORIO COMUNALE DI ..... AGGIORNAMENTO 2010
(Approvato con deliberazione di C.C. N° .... del .....)

INDICE

CAPO I
PRINCIPI GENERALI
Art. 1 - Oggetto
Art. 2 - Definizioni
Art. 3 - Finalità
Art. 4 - Trattamento dei dati personali

CAPO II
OBBLIGHI PER IL TITOLARE DEL TRATTAMENTO
Art. 5 - Notificazione
Art. 6 - Responsabile
Art. 7 - Persone autorizzate ad accedere alla sala di controllo
Art. 8 - Nomina degli incaricati e dei preposti gestione dell'impianto di videosorveglianza
Art. 9 - Accesso ai sistemi e parola chiave

CAPO III
TRATTAMENTO DEI DATI PERSONALI
Sezione I – Raccolta e requisiti dei dati personali
Art. 10 - Modalità di raccolta e requisiti dei dati personali
Art. 11 - Obbligo degli operatori
Art. 12 - Informazioni rese al momento della raccolta

Sezione II – Diritti dell'interessato nel trattamento dei dati
Art. 13 - Diritti dell'interessato

Sezione III – Sicurezza nel trattamento dei dati, limiti alla utilizzabilità dei dati e risarcimento dei danni
Art. 14 - Sicurezza dei dati
Art. 15 - Cessazione del trattamento dei dati
Art. 16 - Limiti alla utilizzazione di dati personali
Art. 17 - Danni cagionati per effetto del trattamento di dati personali

Sezione IV – Comunicazione e diffusione dei dati
Art. 18 - Comunicazione

CAPO IV
TUTELA AMMINISTRATIVA E GIURISDIZIONALE
Art. 19 - Tutela

CAPO V
MODIFICHE
Art. 20 - Modifiche regolamentari

CAPO I
PRINCIPI GENERALI
Art. 1 – Oggetto e norme di riferimento

1. Il presente regolamento disciplina il trattamento dei dati personali, realizzato mediante l'impianto di videosorveglianza cittadina, attivato nel territorio urbano del Comune di .....
2. Per tutto quanto non è dettagliatamente disciplinato nel presente regolamento, si rinvia a quanto disposto dal Codice in materia di protezione dei dati personali approvato con Decreto Legislativo 30 giugno 2003, n. 196 e al Provvedimento Garante Privacy in materia di videosorveglianza 8 aprile 2010.
3. Vengono osservate i principi dal Regolamento sulla videosorveglianza del 2004, circolare Capo della Polizia nr. 558/A/421.2/70/456 del febbraio 2005, circolare del Capo della Polizia nr. 558/A/421.2/70/195960 del 6 agosto 2010.

ART. 2 - Definizioni

1. Ai fini del presente regolamento si intende:

a) per "**banca dati**", il complesso di dati personali, formatosi presso la sala di controllo e trattato esclusivamente mediante riprese video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto;
b) per "**trattamento**", tutte le operazioni o complesso di operazioni, svolte con l'ausilio dei mezzi elettronici, informatici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, l'eventuale diffusione, la cancellazione e la distribuzione di dati;
c) per "**dato personale**", qualunque informazione relativa a persona fisica, persona giuridica, Ente o associazione, identificati o identificabili anche direttamente, e rilevati con trattamenti di immagini effettuati attraverso l'impianto di videosorveglianza;
d) per "**titolare**", l'Ente Comune di ....., nelle sue articolazioni interne, cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali;
e) per "**responsabile**", la persona fisica, legata da rapporto di servizio al titolare e preposto dal medesimo al trattamento dei dati personali;
f) per "**incaricat**i", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
g) per "**interessato**", la persona fisica, la persona giuridica, l'Ente o associazione cui si riferiscono i dati personali;

h) per “**comunicazione**”, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall’interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
i) per “**diffusione**”, il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
l) per “**dato anonimo**”, il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
m) per “**blocco**”, la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.

ART. 3 – Finalità

1. Il presente regolamento garantisce che il trattamento dei dati personali, effettuato mediante l’attivazione di un impianto di videosorveglianza nel territorio urbano, gestito dal Comune di ..... - Corpo di Polizia Municipale e collegato alla centrale operativa della stessa Polizia Municipale nonché a quella della Questura di ....., si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all’identità personale. Garantisce, altresì, i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento. Il sistema informativo e i programmi informatici sono configurati riducendo al minimo l’utilizzazione dei dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzati mediante dati anonimi od opportune modalità che permettano di identificare l’interessato solo in caso di necessità.
2. Presso la centrale operativa della Polizia Municipale e della Questura sono posizionati monitor per la visione in diretta delle immagini riprese dalle telecamere.

Art. 4 - Trattamento dei dati personali

1. Il trattamento dei dati personali è effettuato a seguito dell’attivazione di un impianto di videosorveglianza.
2. Le finalità istituzionali del suddetto impianto sono del tutto conformi alle funzioni istituzionali demandate al Comune di ....., in particolare dal D.lgs.18 agosto 2000 n. 267, dal D.P.R. 24 luglio 1977, n.616, dal D.Lgs.31 marzo 1998, dalla legge 7 marzo 1986 n. 65, sull’ordinamento della Polizia Municipale, nonché dallo statuto e dai regolamenti comunali.

La disponibilità tempestiva di immagini presso il Comando della Polizia Municipale e della Questura di ..... costituisce, inoltre, uno strumento di prevenzione e di razionalizzazione dell'azione delle pattuglie della Polizia Municipale e della Polizia di Stato sul territorio comunale, in stretto raccordo con le altre forze dell'ordine.

3. Gli impianti di videosorveglianza, in sintesi, sono finalizzati:
   a) a prevenire e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e quindi ad assicurare maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana", così individuata secondo il Decreto Ministro Interno 5 agosto 2008;
   b) a tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale e a prevenire eventuali atti di vandalismo o danneggiamento;
   c) al controllo di determinate aree;
   d) al monitoraggio del traffico;
   e) tutelando in tal modo coloro che più necessitano di attenzione: bambini, giovani e anziani, garantendo un elevato grado di sicurezza nelle zone monitorate.
4. Il sistema di videosorveglianza comporterà esclusivamente il trattamento di dati personali rilevati mediante le riprese video e che, in relazione ai luoghi di installazione delle videocamere, interessano i soggetti ed i mezzi di trasporto che transiteranno nell'area interessata.
5. Gli impianti di videosorveglianza non potranno essere utilizzati, in base all'art. 4 dello statuto dei lavoratori (legge 300 del 20 maggio 1970) per effettuare controlli sull'attività lavorativa dei dipendenti dell'amministrazione comunale, di altre amministrazioni pubbliche o di altri datori di lavoro, pubblici o privati. Gli impianti di videosorveglianza non potranno essere utilizzati per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati o per finalità di promozione turistica.

CAPO II
OBBLIGHI PER IL TITOLARE DEL TRATTAMENTO

Art. 5 – Notificazione

1. Il Comune di ....., nella sua qualità di titolare del trattamento dei dati personali, rientrante nel campo di applicazione del presente regolamento, adempie agli obblighi di notificazione preventiva al Garante per la protezione dei dati personali, qualora ne ricorrano i presupposti, ai sensi

e per gli effetti degli artt. 37 e 38 del Codice in materia di protezione dei dati personali approvato con decreto legislativo 30/6/2003, n. 196.

Art. 6 - Responsabile

1. Il Comandante della Polizia Municipale in servizio, o altra persona nominata dal Sindaco, domiciliati in ragione delle funzioni svolte in ..... presso il Comando della Polizia Municipale, è individuato, previa nomina da effettuare con apposito decreto del Sindaco, quale responsabile del trattamento dei dati personali rilevati, ai sensi per gli effetti dell'art. 2, lett. e). E' consentito il ricorso alla delega scritta di funzioni da parte del designato, previa approvazione del Sindaco.
2. Il responsabile deve rispettare pienamente quanto previsto, in tema di trattamento dei dati personali, dalle leggi vigenti, ivi incluso il profilo della sicurezza e dalle disposizioni del presente regolamento.
3. Il responsabile procede al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 1 e delle proprie istruzioni.
4. I compiti affidati al responsabile devono essere analiticamente specificati per iscritto, in sede di designazione.
5. Gli incaricati del materiale trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del titolare o del responsabile.
6. Il responsabile custodisce le chiavi per l'accesso ai locali della centrale di controllo, le chiavi degli armadi per la conservazione delle videocassette/cd o altro supporto informatico, nonché le parole chiave per l'utilizzo dei sistemi.

Art. 7 - Persone autorizzate ad accedere alla sala di controllo

1. L'accesso alla sala di controllo è consentito solamente, oltre al Sindaco o suo delegato, al personale in servizio del Corpo di Polizia Municipale autorizzato dal Comandante e agli incaricati addetti ai servizi, di cui ai successivi articoli.
2. Eventuali accessi di persone diverse da quelli innanzi indicate devono essere autorizzati, per iscritto, dal Comandante del Corpo di Polizia Municipale.
3. Possono essere autorizzati all'accesso alla centrale operativa solo incaricati di servizi rientranti nei compiti istituzionali dell'ente di appartenenza e per scopi connessi alle finalità di cui al presente rego-

lamento, nonché il personale addetto alla manutenzione degli impianti ed alla pulizia dei locali, i cui nominativi dovranno essere comunicati per iscritto al Comandante del Corpo di Polizia Municipale.
4. Il Responsabile della gestione e del trattamento impartisce idonee istruzioni atte ad evitare assunzioni o rilevamento di dati da parte delle persone autorizzate all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali.
5. Gli incaricati dei servizi di cui al presente regolamento vigilano sul puntuale rispetto delle istruzioni e sulla corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.

Art. 8 - Nomina degli incaricati e dei preposti alla gestione dell'impianto di videosorveglianza

1. Il responsabile, designa e nomina i preposti in numero sufficiente a garantire la gestione del servizio di videosorveglianza nell'ambito degli operatori di Polizia Municipale.
2. I preposti andranno nominati tra gli Ufficiale ed Agenti in servizio presso la Centrale Operativa e nei vari settori operativi del Corpo di Polizia Municipale che per esperienza, capacità ed affidabilità forniscono idonea garanzia nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.
3. La gestione dell'impianto di videosorveglianza è riservata agli organi di Polizia Municipale, aventi qualifica di Ufficiali ed Agenti di Polizia Giudiziaria ai sensi dell'art. 55 del Codice di Procedura Penale.
4. Con l'atto di nomina, ai singoli preposti saranno affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi.
5. In ogni caso, prima dell'utilizzo degli impianti, essi saranno istruiti al corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente regolamento.
6. Nell'ambito degli incaricati, verranno designati, con l'atto di nomina, i soggetti cui è affidata la custodia e conservazione delle password e delle chiavi di accesso alla sala operativa ed alle postazioni per l'estrapolazione delle immagini.

Art. 9 - Accesso ai sistemi e parole chiave

1. L'accesso ai sistemi è esclusivamente consentito al responsabile, ai preposti come indicato nei punti precedenti.
2. Gli incaricati ed i preposti saranno dotati di propria password di accesso al sistema.
3. Il sistema dovrà essere fornito di "log" di accesso, che saranno conservati per la durata di anni uno.

CAPO III
TRATTAMENTO DEI DATI PERSONALI

Sezione I
RACCOLTA E REQUISITI DEI DATI PERSONALI

Art. 10 - Modalità di raccolta e requisiti dei dati personali

1. I dati personali oggetto di trattamento sono:
a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per le finalità di cui al precedente art. 4 e resi utilizzabili in altre operazioni del trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi, esatti e, se necessario, aggiornati;
c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
d) conservati per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto, per le quali essi sono stati raccolti o successivamente trattati ed in ogni caso pari al periodo di tempo stabilito dal successivo comma 3;
e) trattati, con riferimento alla finalità dell'analisi dei flussi del traffico, di cui al precedente art.4, comma 3, lett. d), con modalità volta a salvaguardare l'anonimato ed in ogni caso successivamente alla fase della raccolta, atteso che le immagini registrate possono contenere dati di carattere personale.
2. I dati personali sono ripresi attraverso le telecamere dell'impianto di videosorveglianza installate sul territorio comunale.
3. Le telecamere di cui al precedente comma 2 consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale, o in bianco/nero in caso contrario. Il titolare del trattamento dei dati personali si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto attivato. I segnali video delle unità di ripresa saranno inviati presso la Centrale Operativa del Comando di Polizia Municipale. In questa sede le immagini saranno visualizzate su monitor e registrate su appositi server. L'impiego del sistema di videoregistrazione è necessario per ricostruire l'evento, per le finalità previste dal presente Regolamento. Le immagini videoregistrate sono conservate per un tempo non superiore a 72 (settantadue) ore successive alla rilevazione, presso la Centrale Operativa anche in caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. In relazione alle capacità di immagazzinamento delle immagini sui server, le immagini riprese in tempo reale sovrascrivono quelle registrate.

Art. 11 - Obblighi degli operatori

1. L'utilizzo del brandeggio da parte degli operatori e degli incaricati al trattamento dovrà essere conforme ai limiti indicati nel presente regolamento.
2. L'utilizzo delle telecamere è consentito solo per il controllo di quanto si svolga nei luoghi pubblici mentre esso non è ammesso nelle proprietà private.
3. Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo ammesso per la conservazione di cui al precedente articolo, solo in caso di effettiva necessità per il conseguimento delle finalità di cui all'art. 4 comma 3 e a seguito di regolare autorizzazione di volta in volta richiesta al Sindaco.
4. La mancata osservanza degli obblighi previsti al presente articolo comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla normativa vigente, di sanzioni amministrative oltre che l'avvio degli eventuali procedimenti penali.

Art. 12 - Informazioni rese al momento della raccolta

1. Il Comune di ....., in ottemperanza a quanto disposto dall'art. 13 del decreto legislativo 30/6/2003 n. 196, si obbliga ad affiggere un'adeguata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere, su cui è riportata la seguente dicitura: " Polizia Municipale - Comune di ..... - Area videosorvegliata . Immagini custodite presso la Polizia Municipale di .....".
2. Il Comune di ....., nella persona del responsabile, si obbliga a comunicare alla comunità cittadina l'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, l'eventuale incremento dimensionale dell'impianto e l'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, ai sensi del successivo art. 15, con un anticipo di giorni dieci, mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale.

Sezione II
DIRITTI DELL'INTERESSATO NEL TRATTAMENTO DEI DATI

Art. 13 - Diritti dell'interessato

1. In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, ha diritto:

a) di ottenere la conferma dell'esistenza di trattamenti di dati che possono riguardarlo;
b) di essere informato sugli estremi identificativi del titolare e del responsabile oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati;
c) di ottenere, a cura del responsabile, senza ritardo e comunque non oltre 15 giorni dalla data di ricezione della richiesta, ovvero di 30 giorni previa comunicazione all'interessato se le operazioni necessarie per un integrale riscontro sono di particolare complessità o se ricorre altro giustificato motivo:

2. la conferma dell'esistenza o meno di dati personali che lo riguardano anche se non ancora registrati e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento; la richiesta non può essere inoltrata dallo stesso soggetto se non trascorsi almeno novanta giorni dalla precedente istanza, fatta salva l'esistenza di giustificati motivi;
3. la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
4. di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.
5. Per ciascuna delle richieste di cui al comma 1, lett. c), n. 1), può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati e comprensivi dei costi del personale, secondo le modalità previste dalla normativa vigente.
6. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
7. Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.
8. Le istanze di cui al presente articolo possono essere trasmesse al titolare o al responsabile anche mediante lettera raccomandata, telefax o posta elettronica o comunicata oralmente, che dovrà provvedere in merito entro e non oltre quindici giorni.
9. Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Sezione III
SICUREZZA NEL TRATTAMENTO DEI DATI, LIMITI ALLA UTILIZZABILITA' DEI DATI E RISARCIMENTO DEI DANNI

Art. 14 - Sicurezza dei dati

1. I dati personali oggetto di trattamento sono custoditi ai sensi e per gli effetti del precedente art. 10, comma 3.
2. L'utilizzo dei videoregistratori impedisce di rimuovere il disco rigido su cui sono memorizzate le immagini.

Art. 15 - Cessazione del trattamento dei dati

1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati personali sono:
   a) distrutti;
   b) conservati per fini esclusivamente istituzionali dell'impianto attivato.

Art. 16 - Limiti alla utilizzabilità di dati personali

1. La materia è disciplinata dall'art. 14 del Codice in materia di protezione dei dati approvato con decreto legislativo 30 giugno 2003 n.196 e successive modificazioni e o integrazioni.

Art. 17 - Danni cagionati per effetto del trattamento di dati personali

1. La materia è regolamentata per l'intero dall'art. 15 del Codice in materia di protezione dei dati approvato con decreto legislativo 30 giugno 2003 n.196 e successive modificazioni e o integrazioni.

Sezione IV
COMUNICAZIONE E DIFFUSIONE DEI DATI

Art. 18 - Comunicazione

1. La comunicazione dei dati personali da parte del Comune di ..... a favore di soggetti pubblici, esclusi gli enti pubblici economici, è ammessa quando è prevista da una norma di legge o regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria ed esclusivamente per lo svolgimento delle funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'art. 19 comma 2 del D.Lgs. 30/6/2003 n. 196.
2. Non si considera comunicazione, ai sensi e per gli effetti del precedente comma, la conoscenza dei dati personali da parte delle persone incaricate ed autorizzate per iscritto a compiere le operazioni del trattamento dal titolare o dal responsabile e che operano sotto la loro diretta autorità.
3. E' in ogni caso fatta salva la comunicazione o diffusione di dati richiesti, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'art. 58, comma 2, del D.Lgs. 30/6/2003 n. 196 per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

CAPO IV
TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Art. 19 - Tutela

1. Per tutto quanto attiene ai profili di tutela amministrativa e giurisdizionale si rinvia integralmente a quanto previsto dagli artt. 100 e seguenti del decreto legislativo 30 giugno 2003 n.196.
2. In sede amministrativa, il responsabile del procedimento, ai sensi e per gli effetti degli artt. 4-6 della legge 7 agosto 1990, n. 241, è il responsabile del trattamento dei dati personali, così come individuato dal precedente art. 6.

CAPO V
MODIFICHE

Art. 20 - Modifiche regolamentari

1. I contenuti del presente regolamento dovranno essere aggiornati nei casi di aggiornamento normativo in materia di trattamento dei dati personali. Gli eventuali atti normativi, atti amministrativi dell'Autorità di tutela della privacy o atti regolamentari generali del Consiglio comunale dovranno essere immediatamente recepiti.
2. Il presente regolamento è trasmesso al Garante per la protezione dei dati personali a Roma, sia a seguito della sua approvazione, sia a seguito dell'approvazione di suoi successivi ed eventuali aggiornamenti.

Allegato:
UBICAZIONE TELECAMERE NEL COMUNE DI .....
2) PIAZZA
3) PIAZZA LATO ....
4) PIAZZA LATO ......
.....

Finito di stampare
nel mese di novembre 2010
presso Società Tipografica Romana
Pomezia – Roma

ISBN 978-88-96280-22-5

INDICE

Presentazione **pagina 3**

Premessa **pagina 5**

Capitolo I – Il Trattamento dei dati personali mediante videosorveglianza **pagina 7**

Capitolo II – Settori specifici **pagina 19**

Capitolo III - Gli adempimenti dei Comuni che intendono installare un impianto di videosorveglianza **pagina 25**

Capitolo IV – Le pronunce del Garante **pagina 29**

Capitolo V – Un pò di Giurisprudenza **pagina 33**

Capitolo VI – Uso della videoripresa nel corso delle indagini di Polizia Giudiziaria **pagina 35**

Capitolo VII – Per concludere **pagina 39**

Allegato A – Provvedimento in materia di videosorveglianza – 8 Aprile 2010 **pagina 43**

Allegato B – Schema di nuovo regolamento per la disciplina della videosorveglianza **pagina 61**

Allegato C – Carta per un utilizzo democratico della Videosorveglianza
European Forum for Urban Security

Allegato D – Linee Guida per i Comuni in materia di Videosorveglianza alla luce del Provvedimento Garante Privacy 8 aprile 2010
ANCI – Garante per la Protezione dei dati personali

Lo studio è stato curato da:

Dott.ssa Anna MAGGIO – già Comandante del Corpo di Polizia Locale del Comune di GRUGLIASCO e membro del Comitato di redazione per la stesura dei quaderni di aggiornamento per la Polizia Locale ora Comandante della Polizia Provinciale di VERONA

Collana edita dalla REGIONE PIEMONTE
ASSESSORATO COMMERCIO, POLIZIA LOCALE, PROMOZIONE della SICUREZZA
Direzione Commercio, Sicurezza e Polizia Locale – SETTORE SICUREZZA E POLIZIA LOCALE

Curata da:
Dr. Stefano BELLEZZA - Dirigente Responsabile del Settore Sicurezza e Polizia Locale della Regione Piemonte

Hanno collaborato a questo numero: Gino SPAMPATTI ed Enzo VARETTO del Settore Sicurezza e Polizia Locale della REGIONE PIEMONTE

Ages Arti Grafiche SRL
Corso Traiano, 124 - 10127 Torino