UNIONE DEI COMUNI LOMBARDA DELLA VALLETTA

REGOLAMENTO PER LA DISCIPLINA DELLA VIDEOSORVEGLIANZA

SUI TERRITORI DEI COMUNI ASSOCIATI DI PEREGO, ROVAGNATE E SANTA MARIA HOE'

(Approvato con Deliberazione dell'assemblea dell'unione n.° 35 del 28/09/2012)

INDICE

CAPO I - PRINCIPI GENERALI
- Articolo 1 - Premessa
- Articolo 2 - Principi generali
- Articolo 3 - Definizioni
- Articolo 4 - Campo di applicazione
- Articolo 5 - Finalità istituzionali dei sistemi di videosorveglianza

CAPO II – NOTIFICAZIONE, TRATTAMENTO E RACCOLTA DEI DATI
- Articolo 6 - Notificazione
- Articolo 7 - Caratteristiche tecniche dell'impianto e dislocazione
- Articolo 8 – responsabile del trattamento dei dati personali e modalità di raccolta
- Articolo 9 - obblighi deli operatori
- Articolo 10-Accertamenti di illeciti e indagini di autorità giudiziarie o di polizia
- Articolo 11-Informazioni rese al momento della racccolta

CAPO III – DIRITTI DELL'INTERESSATO NEL TRATTAMENTO DEI DATI
- Articolo 12-Diritti dell'interessato
- Articolo 13-sistemi integrati di videosorveglianza
- Articolo 14-ulteriori avvertenze per i sistemi di videosorveglianza posti in essere da enti pubblici

CAPO IV - SICUREZZA NEL TRATTAMENTO DEI DATI, LIMITI ALLA UTILIZZABILITA' DEI DATI E RISARCIMENTO DEI DANNI
- Articolo 15-Sicurezza dei dati
- Articolo 16-Istituti scolastici
- Articolo 17-Deposito dei rifiuti
- Articolo 18-Cessazione del trattamento dei dati
- Articolo 19-Limiti alla utilizzabilità di dati personali
- Articolo 20-Danni cagionati per effetto del trattamento di dati personali

CAPO V – COMUNICAZIONE E DIFFUSIONE DEI DATI
- Articolo 21-comunicazione

CAPO VI – TUTELA AMMINISTRATIVA E GIURISDIZIONALE
- Articolo 22 - Tutele
- Articolo 23 – modifiche regolamentari

CAPO I

Art. 1 – Premessa

Il presente regolamento disciplina il trattamento dei dati personali per mezzo di impianti di videosorveglianza dei comuni aderenti all'Unione dei Comuni Lombarda della Valletta, (di seguito "Unione") determinandone le condizioni necessarie per la tenuta in esercizio ai sensi del DLgs n. 196/2003 e successive modificazioni e integrazioni e in osservanza delle disposizioni contenute nei codici di deontologia promossi dal garante quali: il "decalogo" del 29/11/2000, il provvedimento del 29/04/2004 e la Deliberazione 8 aprile 2010 (10A05072) pubblicata in Gazzetta Ufficiale nr. 99 del 29/04/2010 e succ. modif.

Per tutto quanto non risulta essere dettagliatamente disciplinato nel presente regolamento, si fa rinvio alla normativa in materia di protezione dei dati personali e ai provvedimenti del Garante in materia di videosorveglianza.

Il presente Regolamento garantisce altresì che il trattamento dei dati personali, effettuato mediante l'attivazione di sistemi di videosorveglianza gestiti ed impiegati sui territori comunali di Perego, Rovagnate e Santa Maria Hoè, 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.

Le immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto a cui si riferiscono, costituiscono, secondo la normativa vigente, *"dati personali"*. La videosorveglianza incide sul diritto delle persone alla propria riservatezza; la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini, configurano una operazione di "trattamento di dati personali".

Art. 2 - Principi generali

Il presente regolamento si conforma ai principi di legge: liceità, necessità, proporzionalità e finalità.

- **Principio di liceità**: il trattamento di dati personali dal parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali ai sensi degli artt. 18-22 del Codice.

- **Principio di necessità**: il sistema di videosorveglianza è configurato per l'utilizzazione al minimo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

- **Principio di proporzionalità**: nel commisurare la necessità del sistema di videosorveglianza al grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggetti a concreti pericoli o per le quali non ricorra una effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento.

- **Principio di finalità**: gli scopi perseguiti devono essere determinati, espliciti e legittimi. Sono pertanto escluse finalità di sicurezza pubblica, prevenzione o accertamento dei reati, che competono ad altri organi. E' consentita la videosorveglianza come misura complementare volta a migliorare la sicurezza all'interno o all'esterno di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, o che hanno lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti

Art. 3 - Definizioni

Ai fini del presente regolamento si intende:

a) per **"banca di dati"** il complesso di dati personali formatosi presso la sala di controllo, e trattato esclusivamente mediante riprese televisive che, in relazione ai luoghi di installazione delle videocamere, riguardano prevalentemente i soggetti che transitano nell'area interessata ed i mezzi di trasporto;

b) per il **"trattamento"**, tutte le operazioni o complesso di operazioni, svolte con l'ausilio dei mezzi elettronici 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"**, si intende, qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione e rilevati con trattamenti di immagini effettuati attraverso l'impianto di videosorveglianza;

d) per **"titolare"** il Comune di Santa Maria Hoè, 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 preposta dal medesimo al trattamento dei dati personali;

f) per **"interessato"**, la persona fisica, la persona giuridica, l'ente o associazione cui si riferiscono i dati personali;

g) per **"comunicazione"**, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

h) per **"diffusione"**, il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

i) 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;

k) per **"blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento.

j) per "**Codice**" il Codice in materia di protezione dei dati personali di cui al D. L.vo 196 del 30 giugno 2003 e sue successive modifiche ed integrazioni

Art. 4 - **Campo di applicazione**

1) Il presente regolamento disciplina il trattamento di dati personali, realizzato o realizzabile mediante l'impianto della videosorveglianza, attivato o attivabile nel territorio urbano del Comune di Perego, Rovagnate e Santa Maria Hoe' e collegato alla sala di controllo ubicata presso la sede del servizio unificato di polizia locale dell'Unione dei Comuni Lombarda della Valletta;

2) la potenziale installazione di monitor per la sola visione delle immagini potrà essere attuata presso la centrale operativa del Comando Provinciale Carabinieri di Lecco, della Compagnia Carabinieri di Merate e/o della Questura di Lecco.

Art. 5 – Finalità istituzionali dei sistemi di videosorveglianza
Iniziative coordinate di controllo del territorio

L'attività di videosorveglianza è svolta per fini istituzionali ed è conforme a quanto previsto dalle leggi, dallo statuto e dai regolamenti vigenti, dal D.L.vo 18 agosto 2000, n. 267, dal D.P.R. 24 luglio 1977, n. 616,

dalla legge sull'ordinamento della Polizia Locale 7 marzo 1986, n. 65, dalla Legge Regionale del n. 4 del 14.04.2003; non ha ad oggetto il trattamento di dati sensibili pur non potendosi escludere che le registrazioni effettuate siano idonee a far risalire a informazioni di cui all'art. 22 del D.LGS. 193/2003 .

L'attività di videosorveglianza non prevede una raccolta di immagini collegata e/o incrociata e/o confrontata con altri particolari dati personali oppure con codici identificativi di carte elettroniche o con dispositivi che rendono identificabile la voce e non prevede digitalizzazione o indicizzazione delle immagini tale da rendere possibile una ricerca automatizzata o nominativa.
In particolare, l'uso di impianti di videosorveglianza è strumento per l'attuazione di un sistema integrato di politiche per la sicurezza urbana.
Gli impianti localizzati o localizzabili sugli ambiti territoriali dei comuni aderenti all'Unione assolvono alle seguenti finalità:

- attivazione di misure di prevenzione e di sicurezza del territorio;
- tutela del patrimonio comunale;
- controllo di determinate aree, in particolare a fini preventivi di danneggiamenti, atti di vandalismo, condotte illecite ed episodi di microcriminalità;
- monitoraggio del traffico;

in particolare:

- controllare eventuali accessi limitati al transito veicolare in determinate zone del territorio comunale a veicoli non autorizzati (allestimenti di campi nomadi con autocaravan in aree industriali);
- garantire la protezione dei beni pubblici e privati**;**
- riprendere le immagini di specifici siti comunali come stazioni ecologiche, aree mercatali, parcheggi, scuole, parchi gioco (specie in periodi giornalieri in cui non risulta possibile il ricorso a sistemi di controllo alternativi – orario notturno o giornate festive);
- presidiare gli accessi degli edifici comunali, dell'uff. postale, della polizia locale (per la presenza di casseforti o locali armeria);
- trasmettere e registrare le sedute del consiglio comunale al fine di documentare l'attività dell'ente.

Il sistema di videosorveglianza comporta il trattamento di dati personali rilevati mediante le riprese televisive o web-cam e che, in relazione ai luoghi di installazione delle telecamere, interessano i soggetti ed i mezzi di trasporto che transitano nell'area interessata.

L'Unione promuove ed attua, per la parte di competenza, politiche di controllo del territorio, integrate con organi istituzionalmente preposti alla sicurezza pubblica. A tal fine l'Unione previa intesa o su richiesta delle autorità di pubblica sicurezza e degli organi di polizia, può disporre l'utilizzo degli impianti comunali di videosorveglianza ai fini di prevenzione e repressione di atti delittuosi. I dati così raccolti vengono utilizzati esclusivamente dalle autorità ed organi anzidetti.

CAPO II
NOTIFICAZIONE, TRATTAMENTO E RACCOLTA DEI DATI

Art. 6 – notificazione

L'Unione nella sua qualità di titolare del trattamento dei dati personali, 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 e ss.mm.ii..

Art. 7 – caratteristiche tecniche dell'impianto e dislocazione

Il sistema si compone di una rete di comunicazione dati, basata su tecnologie miste e di telecamere connesse alla sala di controllo posta presso il comando di polizia locale dell'Unione con sede in Santa Maria Hoe' – Piazza Mercato, 3.

Il sistema è a circuito chiuso e i relativi elaboratori non sono interconnessi con altri sistemi, archivi o banche dati, né accessibili da altre periferiche.
L'accesso alle immagini è consentito solamente al responsabile della gestione e del trattamento e agli incaricati addetti ai servizi di cui al successivo articolo. Eventuali accessi di soggetti diversi da quelli innanzi indicati devono essere autorizzati per iscritto dal responsabile.
Nei locali del comando di polizia locale è tenuto il registro degli accesi, su cui saranno annotate, a cura di uno degli incaricati, l'identità della persona, gli orari di entrata e uscita e quant'altro necessario all'identificazione del soggetto, dello scopo dell'accesso, dei dati eventualmente assunti e la sottoscrizione dell'incaricato che ha effettuato la vigilanza.

Art. 8 – responsabile del trattamento dei dati personali e modalità di raccolta

Il responsabile del servizio della polizia locale dell'Unione è designato "responsabile" del trattamento dei dati personali rilevati. E' consentito il ricorso alla delega scritta di funzioni da parte del designato.

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

Il responsabile procede al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, esercita un potere di vigilanza sulla puntuale osservanza delle disposizioni normative o regolamentari in materia.

I compiti affidati al responsabile devono essere analiticamente specificati per iscritto in sede di designazione. Gli incaricati del materiale trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del titolare o del responsabile.

Compete al responsabile per il trattamento designare per iscritto, ed in numero limitato, tutte le persone fisiche incaricate del trattamento dei dati, dell'utilizzazione degli impianti e, nei casi in cui risulta indispensabile per gli scopi perseguiti, della visione delle registrazioni.

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. 5 e resi utilizzabili in altre operazioni del trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi;

b) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;

c) conservati per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto per le quali esse sono state raccolte o successivamente trattate e comunque, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o servizi, nonché nel caso in cui si deve adire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria per un periodo di tempo non superiore a giorni sette. L'eventuale allungamento dei tempi di conservazione deve essere valutato come eccezionale e comunque in relazione alla necessità derivante da un evento già accaduto o realmente incombente, oppure alla necessità di custodire o consegnare una copia specificamente richiesta all'autorità giudiziaria o di polizia giudiziaria in relazione ad un'attività investigativa in corso.

Il software sarà configurato in modo da cancellare, trascorsi i termini sopraindicati, automaticamente i dati registrati.

Le aree in cui verranno installate le telecamere sono identificate mediante atto deliberativo di giunta che ne motiverà la scelta, evitando aree o attività che non sono soggette a concreti pericoli o per le quali non ricorra un'effettiva esigenza di deterrenza o per fini legittimamente perseguibili. Dovranno essere previsti

diversi livelli di accesso al sistema e di utilizzo delle informazioni, attraverso una “doppia chiave” fisica o logica che consenta una immediata ed integrale visione delle immagini solo in caso di necessità.

I dati devono essere protetti da idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, perdita, anche accidentale, di accesso non autorizzato, trattamento non consentito o non conforme alle finalità di raccolta.

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 di cui al precedente art. 5. I segnali video delle unità di ripresa saranno raccolti da una stazione di monitoraggio e controllo presso la sala controllo delle sede della Polizia Locale dell’Unione dei Comuni Lombarda della Valletta. In questa sede le immagini saranno visualizzate su monitor e registrate su un supporto magnetico. L’impiego del sistema di videoregistrazione è necessario per ricostruire l’evento, quando la sala di controllo non è presidiata.

Le attività di videosorveglianza sono finalizzate alla tutela della sicurezza urbana e alla luce delle recenti disposizioni normative, 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 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.

Articolo 9 - Obblighi degli operatori

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.

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. 3 comma 2 e a seguito di regolare autorizzazione di volta in volta richiesta al responsabile del trattamento dei dati personali designato.

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.

Articolo 10 - Accertamenti di illeciti e indagini di autorita’ giudiziarie o di polizia

Ove dovessero essere rilevate immagini di fatti identificativi di ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica o della tutela ambientale e del patrimonio, l’incaricato od il responsabile della videosorveglianza provvederà a darne immediata comunicazione agli organi competenti.
In tali casi, in deroga alla puntuale prescrizione delle modalità di ripresa di cui al precedente articolo 7, l’incaricato procederà alla registrazione delle stesse su supporti magnetici.
Alle informazioni raccolte ai sensi del presente articolo possono accedere solo gli organi di polizia e l’autorità giudiziaria.
L’apparato di videosorveglianza potrà essere utilizzato anche in relazione ad indagini disposte dall’autorità giudiziaria, di organi di polizia o di polizia locale.

Nel caso in cui gli organi di polizia, nello svolgimento di loro indagini, necessitino di avere informazioni ad esse collegate che sono contenute nelle riprese effettuate, possono farne richiesta scritta e motivata indirizzata al responsabile della gestione e del trattamento dei dati.

Articolo 11 Informazioni rese al momento della raccolta

La presenza di un impianto di videosorveglianza deve essere resa pubblica a cura del responsabile dell'impianto, attraverso i mezzi che si riterranno più idonei ed in particolare attraverso:

1. l'affissione del presente regolamento e del nominativo del responsabile dell'impianto all'albo pretorio dell'unione dei comuni lombarda della valletta e del comune in cui è localizzato l'impianto.
2. L'affissione in modo stabile all'albo pretorio degli enti di cui al punto precedente, dell'elenco aggiornato delle posizioni delle telecamere, del loro raggio di azione e delle inquadrature registrate;

un'adeguata segnaletica permanente, nelle strade e nelle piazze e nei luoghi in cui sono posizionate le telecamere, su cui è riportata la seguente dicitura: *"Area videosorvegliata – La registrazione è effettuata dal Comando di Polizia Locale per fini di sicurezza urbana art. 13 del codice in materia di protezione dei dati personali (D.Lg. n. 196/2003* - deliberazione 8 aprile 2010 (10A05072) relativa al provvedimento del Garante in materia di videosorveglianza pubblicato in Gazzetta Ufficiale nr. 99 del 29/04/2010). Il supporto con l'informativa dovrà essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti.

CAPO III
DIRITTI DELL'INTERESSATO NEL TRATTAMENTO DEI DATI

Articolo 12 - Diritti dell'interessato

1) In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, ha diritto:

a) di conoscere l'esistenza di trattamenti di dati che possono riguardarlo;

c) 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;

d) di ottenere, a cura del responsabile, senza ritardo e comunque non oltre 15 giorni dalla data di ricezione della richiesta:

1. 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;
2. 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;
3. di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

2) Per ciascuna delle richieste di cui al comma precedente, può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un rimborso spese, equivalente ai costi effettivamente sopportati e comprensivi dei costi del personale, definiti con atto formale dalla Giunta secondo le modalità previste dalla normativa vigente.

3) 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.

4) 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.

5) 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 verbalmente, che dovrà provvedere in merito entro e non oltre quindici giorni.

6) 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.

7) 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).

Articolo 13 - Sistemi integrati di videosorveglianza

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 citato provvedimento del Garante. Tale collegamento deve essere altresì reso noto nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati .

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 del citato provvedimento del Garante, 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.

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 al Garante.

Articolo 14 - ulteriori avvertenze per i sistemi di videosorveglianza posti in essere da enti pubblici

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.
E' stato individuato al punto 4.6 del citato provvedimento del Garante 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.

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 al Garante, 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 del citato provvedimento del Garante 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).

CAPO IV
SICUREZZA NEL TRATTAMENTO DEI DATI, LIMITI ALLA UTILIZZABILITA' DEI DATI E RISARCIMENTO DEI DANNI

Articolo 15 – sicurezza dei dati

1) I dati personali oggetto di trattamento sono custoditi presso la sala controllo del Comando della Polizia Locale e presso le postazioni fisse dislocate sul territorio di cui all'elenco allegato al presente regolamento, dove sono custoditi i videoregistratori digitali; può accedervi, oltre il Sindaco o suo delegato, solo ed esclusivamente il personale in servizio della Polizia Locale, debitamente istruito sull'utilizzo dell'impianto e debitamente incaricato ed autorizzato per iscritto dal Responsabile individuato o suo delegato, nella loro

qualità di Responsabile del trattamento dei dati personali ad effettuare le operazioni del trattamento dei dati.

2) La sala di controllo è sistematicamente chiusa ed è ubicata negli uffici della Polizia Locale e non accessibile al pubblico nella parte adibita al controllo.

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

4) I dati raccolti mediante sistemi di videosorveglianza dovranno 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). Dovranno 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).

Le misure minime di sicurezza dovranno rispettare i seguenti principi:

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 potranno 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).

A norma delle disposizioni emanate dal Garante si stabilisce che 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.

Si dovrà trattare di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni, individuando altresì 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.).

Articolo 16 - Istituti Scolastici

Il sistema di videosorveglianza attivabile presso istituti scolastici, dovrà 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.

In tale quadro, potrà 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.

E' vietato, altresì, 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 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.

Articolo 17 - Il deposito dei rifiuti

In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l'utilizzo di sistemi di videosorveglianza risulta consentito 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).

Articolo 18 - **Cessazione del trattamento dei dati**

1) In caso di cessazione, per qualsiasi causa, di un trattamento i dati personali sono:
   a) distrutti;
   b) ceduti ad altro titolare purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
   c) conservati per fini esclusivamente istituzionali dell'impianto attivato.

2) La cessione dei dati in violazione di quanto previsto dal comma precedente lett. b) o di altre disposizioni di legge in materia di trattamento dei dati personali è priva di effetti. Sono fatte salve le sanzioni previste dalla legge.

Articolo 19 - Limiti alla utilizzabilità di dati personali

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 della deliberazione 8 aprile 2010 (10A05072) relativa al provvedimento del Garante in materia di videosorveglianza pubblicato in Gazzetta Ufficiale nr. 99 del 29/04/2010.

Articolo 20 - Danni cagionati per effetto del trattamento di dati personali

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 della deliberazione 8 aprile 2010 (10A05072) relativa al provvedimento del Garante in materia di videosorveglianza pubblicato in Gazzetta Ufficiale nr. 99 del 29/04/2010

CAPO V
COMUNICAZIONE E DIFFUSIONE DEI DATI

Articolo 21 - Comunicazione

1) La comunicazione dei dati personali da parte dell'Unione 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 decreto legislativo 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.

CAPO VI
TUTELA AMMINISTRATIVA E GIURISDIZIONALE

Articolo 22 - Tutele

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 e loro.

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

CAPO VII
MODIFICHE

Articolo 23 - Modifiche regolamentari

1) I contenuti del presente regolamento dovranno essere aggiornati nei casi di adeguamento normativo in materia di trattamento dei dati personali. Gli eventuali atti normativi, atti amministrativi dell'Autorità di tutela della privacy o atti regolamentari generali dell'assemblea dell'Unione.

2) All'aggiornamento degli indirizzi vincolanti provvederà la giunta dell'unione ai sensi e per gli effetti di quanto previsto dal vigente ordinamento delle autonomie locali.

3) L'approvazione del presente regolamento abroga e sostituisce, a tutti gli effetti di legge, ogni regolamento approvato in data anteriore.