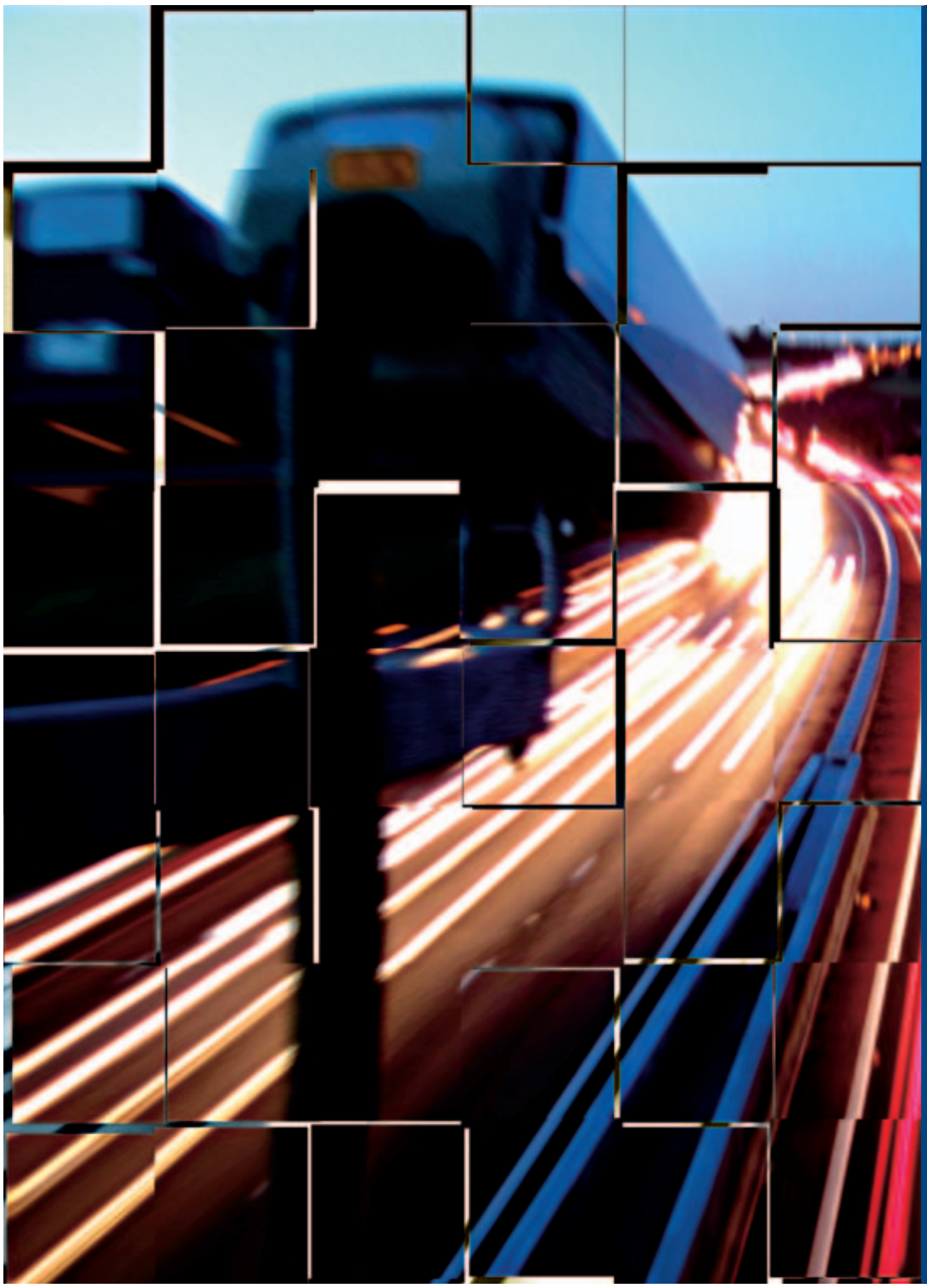
I SISTEMI DI VIDEOSORVEGLIANZA 2

Videosorveglianza e privacy: quadro normativo, casistica e aspetti tecnici



PROVINCIA AUTONOMA DI TRENTO

TRANSCRIME

*info*sicurezza 4

UNIVERSITÀ DEGLI STUDI DI TRENTO

UNIVERSITÀ CATTOLICA DEL SACRO CUORE

*info*sicurezza 4

Provincia autonoma di Trento
Transcrime – università di trento e università cattolica di milano

I SISTEMI DI VIDEOSORVEGLIANZA 2

VIDEOSORVEGLIANZA E PRIVACY: QUADRO NORMATIVO, CASISTICA E ASPETTI TECNICI

Giunta della Provincia autonoma di Trento

Maggio 2006

Giunta della Provincia autonoma di Trento
ISBN 88-7702-143-8

Collana ***info***sicurezza 4
Assessorato alle opere pubbliche, protezione civile e autonomie locali
Sistema integrato di sicurezza nel Trentino
Servizio autonomie locali
e-mail: serv.autonomielocali@provincia.tn.it
www.autonomielocali.provincia.tn.it

I sistemi di videosorveglianza 2
Videosorveglianza e privacy:
quadro normativo, casistica e aspetti tecnici

A cura di
Ernesto U. Savona e Stefano Caneppele
TRANSCRIME Università degli Studi di Trento –
Università Cattolica del Sacro Cuore
www.transcrime.unitn.it

Collaborazione
Ufficio Stampa – Provincia autonoma di Trento
Coordinamento editoriale
Silvia Vernaccini
Impaginazione
Gabriele Weber
Stampa
Lineagrafica Bertelli Editori – Trento

Editore
Provincia autonoma di Trento

Stesura del testo
a cura di

Stefano Caneppele
TRANSCRIME Università degli Studi di Trento
Università Cattolica del Sacro Cuore
(Premessa e revisione generale)

Roberto Caso
Università degli Studi di Trento
(Parte A e B)

Francesco De Natale
DIT – Dipartimento Informatica e Telecomunicazioni dell'Università degli Studi di Trento
(Parte C)

PRESENTAZIONE

La guida *Videosorveglianza e privacy* è la seconda tappa, nel contesto del Sistema integrato di sicurezza della Provincia autonoma di Trento, del percorso che la Provincia di Trento ha avviato nel 2003 con il progetto "Tecnologie per la sicurezza". La filosofia di fondo è stata, fin dall'inizio, quella di indagare quanto le nuove tecnologie, la videosorveglianza in particolare, potessero contribuire alla riduzione dei comportamenti criminali con una costante attenzione a un corretto bilanciamento tra l'esigenza di sicurezza e il rispetto della privacy dei cittadini.
Nel contesto italiano sono ormai evidenti due tendenze: da un lato, si registra negli ultimi anni un aumento nella diffusione della videosorveglianza; dall'altro si sta diffondendo la consapevolezza, evidenziata da diverse ricerche, che questo strumento può essere di aiuto in alcuni casi, di nessuno in altri. Riteniamo perciò di primaria importanza la sensibilizzazione degli operatori locali a un utilizzo 'ragionato' delle nuove tecnologie, che miri contemporaneamente all'efficacia e all'efficienza. Proprio questa riflessione, che ha mosso i primi passi nel 2004 con la pubblicazione della prima guida *I sistemi di videosorveglianza*, ha aperto la strada al tema portante di questa seconda edizione, ovvero il rapporto tra videosorveglianza e privacy.
La guida fornisce in primo luogo una dettagliata presentazione del quadro normativo in materia di privacy, soffermandosi sui quattro principi cardine che devono guidare ogni trattamento dei dati (liceità, necessità, proporzionalità, finalità). Successivamente l'attenzione si sposta sulle procedure che i soggetti pubblici sono tenuti a seguire in alcuni casi specifici, quali il controllo del traffico e degli spazi pubblici, degli istituti scolastici e dei luoghi di culto, dei luoghi di lavoro ecc. Per finire, si affrontano alcuni aspetti tecnici, quali la conservazione e l'utilizzo del materiale raccolto, il tempo di vita dei dati, l'uso legale e la marchiatura di questi. Crediamo che solo fornendo agli operatori pubblici una continua e approfondita conoscenza del tema si possano garantire scelte equilibrate capaci di dare ai cittadini sicurezza, rispettando il loro inviolabile diritto alla riservatezza.

Silvano Grisenti
Assessore alle Autonomie Locali
Provincia autonoma di Trento

INDICE

PREMESSA

La videosorveglianza ha registrato negli ultimi anni una diffusione senza precedenti in tutti i paesi occidentali. Dopo l'11 settembre 2001 gli investimenti nel settore dell'*information and communication technology* (ICT) evidenziano un trend di crescita che non pare destinato ad arrestarsi neppure nei prossimi anni[1]. Nei fatti, la lotta al terrorismo si è tradotta in una ridefinizione di priorità, obiettivi e strumenti da parte delle agenzie nazionali di controllo formale che ha portato a incentivare sensibilmente l'impiego delle nuove tecnologie. Gli effetti di questa novità si sono fatti sentire anche a livello locale, con una diffusione su larga scala dei sistemi di videosorveglianza.

Negli ultimi anni, anche in Italia, le politiche di sicurezza degli enti locali hanno fatto ricorso allo strumento della videosorveglianza. Le telecamere sono spesso diventate l'unico intervento di prevenzione situazionale generalmente adottato per ridurre ogni forma di criminalità[2].
Il messaggio diretto all'opinione pubblica è stato "+ telecamere = + prevenzione dei reati = – criminalità". Quanto questo corrisponda al vero è difficile dirlo, almeno per l'Italia. In Inghilterra gli studi più recenti pubblicati (Gill, Spriggs, 2005) non paiono confermare – almeno in linea generale – questa indicazione[3]. Nonostante ciò, l'opinione pubblica tende a mantenere un'alta fiducia nel potere deterrente dell'"occhio tecnologico". Lo scambio tra (più) sicurezza e (meno) privacy è oggi accettato senza troppe resistenze[4].

[1] Secondo alcune stime (Freedonia Group) il mercato mondiale della sicurezza e della videosorveglianza elettronica cresce ogni anno dell'8,4% e raggiungerà nel 2008 i 74 miliardi di dollari (circa 150 mila miliardi di vecchie lire).

[2] Il che è in sé – a pensarci – un paradosso in quanto per definizione queste misure sono fisiologicamente situazionali, ossia legate al contesto in cui una specifica categoria di reati si sviluppa (Clarke R.V. (1997), *Situational Crime Prevention: Successful Case Studies*, Harrow & Heston, New York).

[3] "Tutti i sistemi CCTV avevano il generico obiettivo di ridurre la criminalità. Su 13 casi analizzati 6 hanno riportato una diminuzione dei livelli di criminalità [...] ma solo in un caso la diminuzione è attribuibile alle CCTV. Nei 7 casi in cui vi è stato l'aumento di criminalità questo non è dipeso dalle CCTV" (Gill M., Spriggs A. (2005), *Assessing the Impact of CCTV*, Home Office Research, Londra, p. vi).

[4] È probabile che alla base di questa fiducia da parte dell'opinione pubblica vi sia un equivoco di fondo che consideri interscambiabili i concetti di funzione di *deterrence* e funzione di *detection* esercitati dalla videosorveglianza. La prima attiene alla capacità dello strumento di prevenire il reato, la seconda attiene alla capacità dello strumento di identificare l'autore del reato, una volta che questo è stato commesso. La prima assolve una funzione tipicamente propria delle politiche di sicurezza locali. La seconda assolve una funzione tipicamente propria delle politiche di sicurezza nazionali. In altre parole, potremmo teorizzare che le telecamere "piacciono" non solo e non tanto perché prevengono i reati, ma in quanto trasmettono, agli occhi dei cittadini, l'idea che "non è più possibile farla franca". Le telecamere si trasformerebbero passando da "guardiani capaci" – come recita la celebre teoria dell'attività di routine – a testimoni affidabili. In molti casi, tuttavia, succede che a mancare sia non solo l'affidabilità ma anche la testimonianza.

Perché i sistemi di videosorveglianza hanno raccolto un così grande successo anche a livello locale? Forse perché nel breve periodo l'adozione di un sistema di videosorveglianza appare *a priori* spesso come la migliore scelta possibile. Ciò per svariate ragioni: a) da un punto di vista della prevenzione, è dimostrato che i primissimi mesi di vita dell'intervento sono quelli che fanno registrare una marcata riduzione della criminalità nell'area interessata; b) da un punto di vista della rassicurazione, l'appoggio dell'opinione pubblica può garantire una crescita del livello di sicurezza dei cittadini (e del consenso negli amministratori); c) da un punto di vista economico, le telecamere paiono quasi sempre rappresentare un investimento efficiente in termini di risorse (soprattutto perché a volte sopperiscono a una mancanza di personale); d) da un punto di vista tecnico, si tratta di interventi che possono essere posti in essere in tempi relativamente brevi (consentendo quindi all'amministratore di fornire una risposta concreta e rapida a un bisogno impellente); e) da un punto di vista della comunicazione, trasmettono l'idea che l'amministrazione si sta impegnando concretamente per ridurre la criminalità.

Nel medio-lungo periodo, però, molti di questi benefici vengono meno. Infatti: a) da un punto di vista della prevenzione molto spesso, dopo alcuni mesi, i livelli di criminalità tendono a riportarsi sui valori precedenti all'intervento o possono comportare una crescita dei livelli di criminalità in altri quartieri cittadini; b) da un punto di vista della rassicurazione, l'appoggio dell'opinione pubblica tende a diminuire; c) da un punto di vista economico, le telecamere risultano essere più costose di quanto previsto (accade spesso che le spese di manutenzione siano inizialmente sottostimate); d) da un punto di vista tecnico, la performance del sistema di videosorveglianza tende a peggiorare nel tempo; e) da un punto di vista della comunicazione, è richiesto un impegno continuativo nel tempo per far risaltare i successi ottenuti dal sistema di videosorveglianza.

L'esperienza inglese, da sempre in prima fila nel settore delle CCTV (*Closed Circuit Television Camera*), può insegnare molto evitando di ripetere in futuro gli errori passati.

La differenza tra il fallimento e il successo di un intervento risiede soprattutto in una ponderata e accorta analisi:

1) delle necessità e dei bisogni del territorio in cui va inserita la misura di prevenzione (sostenibilità sociale)[5];

[5] Ad esempio si è visto che la promozione di un bando governativo di finanziamento per l'acquisto di CCTV – se generico nei requisiti – può favorire la presentazione di progetti poco qualificati o mal congegnati nell'analisi del territorio, presentati solo perché vi è la possibilità di ricevere un finanziamento e non sulla base di reali esigenze di prevenzione. Questo suggerisce agli enti co-finanziatori di sistemi di videosorveglianza di prevedere per i bandi procedure di verifica che en-

2) della misura di prevenzione più appropriata a massimizzare i benefici e a ridurre i costi per la collettività (sostenibilità economica)[6];

3) delle necessità e dei bisogni che ha la misura di prevenzione per poter funzionare nel migliore dei modi (sostenibilità organizzativa)[7].

Ciò significa che è necessaria una conoscenza dei problemi, degli strumenti e del loro funzionamento. Più la conoscenza di questi tre elementi è confusa più aumentano le probabilità di insuccesso. In questo senso le norme dettate in materia di privacy possono rappresentare un utile strumento per favorire un utilizzo ragionevole dei sistemi di CCTV che – come ricorda l'Autorità Garante della privacy – vanno utilizzati solo come *extrema ratio*, cioè solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili.
La videosorveglianza può essere di molto aiuto in alcuni casi, di nessuno in altri. Occorre lavorare nella direzione di costruire una sensibilità comune tra gli operatori locali per favorire sempre più un utilizzo efficace e efficiente delle risorse pubbliche investite in questo settore.

trino nel merito del progetto, del suo disegno, dei suoi presupposti e della sua valutazione. Indica inoltre l'opzione di incentivare la raccolta e l'analisi, in via continuativa, di dati statistici a livello locale.

[6] In Inghilterra diversi progetti di videosorveglianza non avevano previsto fondi per la formazione del personale, per la gestione dell'impianto e neppure ipotizzato costi di manutenzione ordinaria e straordinaria della strumentazione tecnica. Ciò suggerisce agli enti locali di non sottovalutare i costi di gestione dei sistemi di videosorveglianza.

[7] Molti dei sistemi di videosorveglianza analizzati dai ricercatori inglesi avevano obiettivi generici, non stabilivano protocolli operativi in caso di detezione di comportamenti criminali e/o sospetti. Inoltre diverse telecamere presentavano immagini sfuocate, di cattiva qualità perché non erano state inizialmente testate. La costruzione dei sistemi di videosorveglianza non può mai essere interamente demandata ad un consulente tecnico esterno. Questi deve essere seguito costantemente dal personale dell'ente locale. L'esempio suggerisce agli enti locali di predisporre verifiche tecniche preliminari sulla strumentazione fornita e di definire in via preventiva dei protocolli operativi nel caso i sistemi di videosorveglianza identificassero situazioni a rischio.

A. LA TEORIA: PRINCIPI E REGOLE

1. INTRODUZIONE

In Italia la normativa in materia di privacy discende dalla convenzione n. 108/1981 del Consiglio d'Europa sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale e dalla direttiva comunitaria 95/46 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Tutela della privacy

Obblighi e diritto alla protezione dei dati personali

In particolare, la direttiva si fonda sul perseguimento di un elevato livello di protezione dei dati personali e sulla "procedimentalizzazione della tutela della privacy".
Sotto quest'ultimo profilo, la normativa comunitaria si caratterizza per il fatto di regolamentare oltre che i diritti dell'interessato anche e soprattutto gli obblighi da parte di chi "tratta i dati personali". A sorvegliare sul rispetto delle prescrizioni normative è posta un'autorità indipendente, in Italia denominata "Garante per la Protezione dei Dati Personali" (d'ora in poi, Garante).

L'Italia ha dato attuazione alla direttiva 95/46 con la legge 675 del 1996, alla quale sono seguite altre leggi e regolamenti. Per mettere ordine in una disciplina sempre più frammentaria è stato emanato il d.lgs. 30 giugno 2003, n. 196, codice in materia di protezione dei dati personali (d'ora in poi, Codice), entrato in vigore il 1° gennaio del 2004. Il Codice, però, non ha solo lo scopo di riordinare la materia, ma anche di rafforzare la tutela dei dati personali e dare attuazione alla direttiva 2002/58 relativa alla vita privata e alle comunicazioni elettroniche. In quest'ottica di rafforzamento si spiega la tutela del nuovo "diritto alla protezione dei dati personali".

La tutela posta dal Codice è assistita da sanzioni penali e amministrative, oltre che da rimedi di carattere civile.
L'esecuzione della tutela è affidata agli organi giurisdizionali e al Garante.

Nell'ambito della materia della privacy, la videosorveglianza occupa uno spazio progressivamente rilevante. L'evoluzione tecnologica rende sempre più potente e sofisticata la videosorveglianza. In particolare, spicca la possibilità di collegare i sistemi di videosorveglianza alla rete Internet.
Tali sistemi, da una parte sono – o sono percepiti, soprattutto dopo gli attentati dell'11 settembre – come fondamentali strumenti di sicurezza, dall'altra sono tecnologie di invasione della privacy.

I sistemi di videosorveglianza appaiono perciò come una delle tecnologie per le quali è più difficile mantenere il necessario equilibrio tra esigenze di sicurezza e esigenze di protezione della privacy.

Proprio al mantenimento di questo equilibrio si è dedicato il Garante, il quale con una serie di provvedimenti di varia natura – decisioni su ricorsi, contestazioni di violazioni amministrative, pareri e provvedimenti generali – ha interpretato e applicato i principi legislativi in materia di protezione dei dati personali al tema della videosorveglianza.

Provvedimento generale del Garante

L'opera interpretativa del Garante è oggi riassunta nel provvedimento generale del 29 aprile 2004, il quale riproduce e adatta al contesto italiano gli indirizzi formulati dalle autorità europee di protezione dei dati riunite nel Gruppo istituito dalla dir. 95/46 (parere 4/2004 relativo al trattamento dei dati personali mediante videosorveglianza adottato l'11 febbraio 2004) e le linee-guida del Consiglio d'Europa del 20-23 maggio 2003.

Altre normative

Sulla materia della videosorveglianza, oltre al Codice, incidono anche altre normative. A titolo di esempio si possono ricordare:

- il d.m. del 6 giugno 2005, modifiche e integrazioni al decreto ministeriale 18 marzo 1996, recante norme di sicurezza per la costruzione e l'esercizio degli impianti sportivi;
- il d.lgs. 4 febbraio 2000, n. 45, attuazione della direttiva 98/18/CE relativa alle disposizioni e alle norme di sicurezza per le navi da passeggeri adibite a viaggi nazionali;
- il d.l. 24 febbraio 2003, n. 28, disposizioni urgenti per contrastare i fenomeni di violenza in occasione di competizioni sportive, convertito, con modificazioni, dalla l. 24 aprile 2003, n. 88;
- il d.p.r. 22 giugno 1999, n. 250, regolamento recante norme per l'autorizzazione alla installazione e all'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato, a norma dell'articolo 7, comma 133-bis, della legge 15 maggio 1997, n. 127;
- il d.l. 14 novembre 1992, n. 433, misure urgenti per il funzionamento dei musei statali, convertito, con modificazioni, dalla legge 14 gennaio 1993, n. 4;
- la l. 20 maggio 1970, n. 300, c.d. statuto dei lavoratori.

Occorre inoltre ricordare che si è in attesa dell'approvazione del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini previsto dall'art. 134 del Codice.

2. Il provvedimento generale del Garante per la Protezione dei Dati Personali del 2004: principi generali

Dato personale

In base all'interpretazione del Garante, il Codice, come già la precedente l. 675/96, considera "dato personale" qualunque informazione che permetta l'identificazione anche in via indiretta dei soggetti interessati, anche quando l'informazione deriva da suoni o da immagini anziché da dati alfanumerici.

Dunque il Codice è certamente applicabile anche ai trattamenti di suoni e di immagini effettuati attraverso sistemi di videosorveglianza, a prescindere dalla circostanza che tali informazioni siano eventualmente registrate in un archivio elettronico e comunicate a terzi, dopo il loro temporaneo monitoraggio in un circuito di controllo.

Il Garante ha precisato che "non è necessario che le persone siano identificate in maniera chiara e univoca, *essendo sufficiente che i soggetti possano essere identificati attraverso, ad esempio, il collegamento con altre fonti conoscitive quali foto segnaletiche, identikit o archivi di polizia contenenti immagini*" (v., tra gli altri, il parere 17 dicembre 1997, Bollettino del n. 2/ agosto 1997, pag. 57).

Principi per il trattamento dei dati personali in caso di videosorveglianza

Il provvedimento generale del 2004 è stato emanato al fine di aggiornare e integrare i principi e le prescrizioni contenuti nel precedente provvedimento generale del 29 novembre del 2000, c.d. "decalogo" per il trattamento dei dati personali mediante videosorveglianza. Il nuovo provvedimento si è reso necessario a seguito dell'emanazione del codice in materia di protezione dei dati personali e delle altre disposizioni che hanno rafforzato le garanzie per i cittadini.

Il provvedimento, nella prima parte, richiama alcuni principi e illustra le prescrizioni generali – adempimenti – relative a tutti i sistemi di videosorveglianza; nella seconda parte, invece, individua le prescrizioni riguardanti specifici trattamenti di dati (ad esempio, quelli effettuati da soggetti pubblici).

I quattro principi generali applicabili a tutti i trattamenti compiuti mediante videosorveglianza sono i seguenti.

Principio di liceità del trattamento dei dati

1) Principio di liceità (art. 11 Codice). Il trattamento dei dati attraverso sistemi di videosorveglianza deve essere fondato su uno dei presupposti di liceità previsti dal Codice, ovvero:
- per gli organi pubblici: svolgimento di funzioni istituzionali (artt. 18-22 Codice);
- per i soggetti privati e gli enti pubblici economici: adempimento di un obbligo di legge, provvedimento del

Garante di c.d. bilanciamento di interessi o consenso libero e espresso (artt. 23-27 Codice).

Inoltre, l'installazione di sistemi di videosorveglianza deve rispettare le altre prescrizioni normative in materia (si veda, ad esempio, l'art. 4 della l. 20 maggio 1970, n. 300, c.d. statuto dei lavoratori, che vieta l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori).

2) Principio di necessità (art. 3 Codice). "Ciascun sistema informativo e il relativo programma informatico vanno 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*. Il software va configurato anche in modo da *cancellare periodicamente* e *automaticamente* i dati eventualmente registrati".

Principio di necessità del trattamento

Esempio: un programma per il monitoraggio del traffico va configurato in modo da consentire solo riprese generali che escludono la possibilità di ingrandire le immagini.

3) Principio di proporzionalità. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano attentamente valutate come insufficienti o inattuabili. "Non va adottata la scelta semplicemente meno costosa, o meno complicata, o di più rapida attuazione, che potrebbe non tener conto dell'impatto sui diritti degli altri cittadini o di chi abbia diversi legittimi interessi". "Il titolare del trattamento, prima di installare un impianto di videosorveglianza, deve valutare, obiettivamente e con un approccio selettivo, se l'utilizzazione ipotizzata sia in concreto realmente proporzionata agli scopi prefissi e legittimamente perseguibili".

Principio di proporzionalità

In applicazione del principio di proporzionalità la videosorveglianza va delimitata rigorosamente:

- anche presso luoghi pubblici o aperti al pubblico, quando sia di legittimo e effettivo interesse per particolari finalità, la ripresa di luoghi privati o di accessi a edifici;
- l'utilizzazione di specifiche soluzioni quali il collegamento ad appositi "centri" cui inviare segnali di allarme sonoro o visivo, oppure l'adozione di interventi automatici per effetto di meccanismi o sistemi automatizzati d'allarme (chiusura accessi, afflusso di personale di vigilanza, ecc.), tenendo anche conto che in caso di trattamenti volti a definire profili o personalità degli interessati il Codice prevede ulteriori garanzie (art. 14, comma 1, del Codice);
- l'eventuale duplicazione delle immagini registrate;
- la creazione di una banca di dati quando, per le finalità perseguite, è sufficiente installare un sistema a circuito

chiuso di sola visione delle immagini, senza registrazione (ad esempio per il monitoraggio del traffico o per il controllo del flusso ad uno sportello pubblico).

La proporzionalità va valutata in ogni fase o modalità del trattamento.

Esempio: il principio di proporzionalità va tenuto in considerazione per stabilire quanto di seguito elencato.

- Se sia sufficiente, ai fini della sicurezza, rilevare immagini che non rendono identificabili i singoli cittadini, anche tramite ingrandimenti;
- se sia realmente essenziale ai fini prefissi raccogliere immagini dettagliate;
- la dislocazione, l'angolo visuale, l'uso di zoom automatici e le tipologie – fisse o mobili – delle apparecchiature;
- quali dati rilevare, se registrarli o meno, se avvalersi di una rete di comunicazione o creare una banca dati, indicizzarla, utilizzare funzioni di fermo-immagine o tecnologie digitali, abbinare altre informazioni o interconnettere il sistema con altri gestiti dallo stesso titolare o da terzi;
- la durata dell'eventuale conservazione (che, comunque, deve essere sempre temporanea).

4) Principio di finalità. Gli scopi perseguiti con il trattamento attuato mediante videosorveglianza devono essere determinati, espliciti e legittimi (art. 11, comma 1, lett. b), del Codice). "Ciò comporta che il titolare possa perseguire solo finalità di sua pertinenza". "In ogni caso, possono essere perseguite solo finalità determinate e rese trasparenti, ossia direttamente conoscibili attraverso adeguate 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 (art. 11, comma 1, lett. b), del Codice). Le finalità così individuate devono essere correttamente riportate nell'informativa".

Principio di finalità

Esempio: il Garante ha constatato che taluni soggetti pubblici e privati si propongono abusivamente, quale scopo della videosorveglianza, finalità di sicurezza pubblica, prevenzione o accertamento dei reati che invece competono solo ad Organi giudiziari o di polizia giudiziaria oppure a Forze armate o di polizia.

3. Il provvedimento generale del Garante per la Protezione dei Dati Personali del 2004: adempimenti

3.1 Informativa

Il Garante ha precisato che "gli interessati devono essere informati che stanno per accedere o che si trovano in una zona videosorvegliata e dell'eventuale registrazione" (v. anche le contestazioni di violazione amministrativa 5 ottobre 2002, Bollettino del n. 32/ottobre 2002, pag. 124; 18 giugno 2002, Bollettino del n. 30/luglio 2002, pag. 156; 2 aprile 2002, Bollettino del n. 27/aprile 2002, pag. 73); "ciò anche nei casi di eventi e in occasione di spettacoli pubblici (concerti, manifestazioni sportive) o di attività pubblicitarie (attraverso web cam)".

Informativa obbligatoria

"L'informativa deve fornire gli elementi previsti dal Codice (art. 13) anche con formule sintetiche, ma chiare e senza ambiguità".

Esempio: il Garante ha individuato ai sensi dell'art. 13, comma 3, del Codice un modello semplificato di informativa "minima", che può essere utilizzato in particolare in aree esterne. Il modello è ovviamente adattabile a varie circostanze. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, vanno installati più cartelli.

"*In luoghi diversi dalle aree esterne* il modello *va integrato* con almeno un avviso circostanziato che riporti gli elementi del predetto art. 13 con particolare riguardo alle finalità e all'eventuale conservazione".

www.istockphoto.com

Il supporto con l'informativa:
- deve essere collocato *nei luoghi ripresi o nelle immediate vicinanze*, non necessariamente a contatto con la telecamera;
- deve avere un formato e un posizionamento tale da essere *chiaramente visibile*;
- può inglobare *un simbolo o una stilizzazione di esplicita e immediata comprensione*, eventualmente diversificati se le immagini sono solo visionate o anche registrate.

3.2 Prescrizioni specifiche

1) Verifica preliminare

Verifica preliminare del Garante

Il Garante ha stabilito che "tutti i titolari del trattamento, quale *misura opportuna* per favorire il rispetto delle previsioni di legge (art. 143, comma 1, lett. c), del Codice), devono sottoporre alla verifica preliminare [del Garante] *i sistemi di videosorveglianza che:*
- prevedono una raccolta delle immagini collegata e/o incrociata e/o confrontata con altri particolari dati personali (ad esempio biometrici), oppure con codici identificativi di carte elettroniche o con dispositivi che rendono identificabile la voce.

La verifica preliminare del Garante *occorre anche:*
- in caso di digitalizzazione o indicizzazione delle immagini (che rendono possibile una ricerca automatizzata o nominativa);
- in caso di videosorveglianza c.d. dinamico-preventiva che non si limiti a riprendere staticamente un luogo, ma rilevi percorsi o caratteristiche fisionomiche (ad esempio riconoscimento facciale) o eventi improvvisi, oppure comportamenti anche non previamente classificati".

2) Autorizzazioni

Autorizzazione del Garante

I trattamenti di dati personali effettuati mediante videosorveglianza "devono essere autorizzati preventivamente dal Garante, anche attraverso autorizzazioni generali, quando riguardano dati sensibili o giudiziari, ad esempio in caso di riprese di persone malate o di detenuti (artt. 26 e 27 del Codice)".

3) Notificazione

Notificazione

I trattamenti di dati a mezzo videosorveglianza "devono essere notificati al Garante solo se rientrano in casi specificamente previsti (art. 37 del Codice)". A tale riguardo lo stesso Garante "ha disposto che *non vanno comunque notificati i trattamenti relativi a comportamenti illeciti o fraudolenti quando riguardano immagini o suoni conservati temporaneamente per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio*

(provv. n. 1/2004 del 31 marzo 2004, in G.U. 6 aprile 2004, n. 81 e in www.garanteprivacy.it; v. anche, sullo stesso sito, i chiarimenti forniti con nota n. 9654/33365 del 23 aprile 2004 relativamente alla posizione geografica delle persone)".

3.3 Soggetti preposti e misure di sicurezza

1) Responsabili e incaricati

"Si devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate ad utilizzare gli impianti e, nei casi in cui è indispensabile per gli scopi perseguiti, a visionare le registrazioni (art. 30 del Codice). Deve trattarsi di un numero molto ristretto di soggetti, in particolare quando ci si avvale di una collaborazione esterna".

Numero ristretto di incaricati designati per iscritto

"La designazione di eventuali responsabili e incaricati "esterni" può essere effettuata *solo se l'organismo esterno svolge prestazioni strumentali e subordinate alle scelte del titolare del trattamento*".

"Quando i dati vengono conservati – naturalmente per un tempo limitato in applicazione del principio di proporzionalità – devono essere previsti *diversi livelli di accesso al sistema e di utilizzo delle informazioni*, avendo riguardo anche ad eventuali interventi per esigenze di manutenzione. Occorre prevenire possibili abusi attraverso opportune misure basate in particolare *su una "doppia chiave" fisica o logica* che consentano una immediata e integrale visione delle immagini solo in caso di necessità (da parte di addetti alla manutenzione o per l'estrazione dei dati ai fini della difesa di un diritto o del riscontro ad una istanza di accesso, oppure per assistere la competente Autorità giudiziaria o di polizia giudiziaria). Va infatti tenuto conto che l'accessibilità regolamentata alle immagini registrate da parte degli addetti è fattore di sicurezza" (v. anche il parere 23 marzo 1999, Bollettino del n. 8/marzo 1999, pag. 57).

2) Misure di sicurezza

"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 o trattamento non consentito o non conforme alle finalità della raccolta (art. 31 del Codice)".

Misure di sicurezza dei dati

Alcune misure, c.d. "misure minime", sono obbligatorie anche sul piano penale (art. 33 del Codice).

"Il titolare del trattamento che si avvale di un soggetto esterno deve ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle regole in

materia (artt. 33-36 e 169, nonché Allegato B) del Codice, in particolare punto 25; v. anche i chiarimenti forniti con nota n. 6588/31884 del 22 marzo 2004, in www.garanteprivacy.it)".

3.4 Durata dell'eventuale conservazione dei dati

In applicazione del principio di proporzionalità (v. anche art. 11, comma 1, lett. e), del Codice), anche l'eventuale conservazione temporanea dei dati deve essere commisurata al grado di indispensabilità e per il solo tempo necessario – e predeterminato – a raggiungere la finalità perseguita.

Conservazione dei dati per il solo tempo indispensabile

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 specifici 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), è ammesso un tempo più ampio di conservazione dei dati, che non può comunque superare la settimana.

Un 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 dall'Autorità giudiziaria o di polizia giudiziaria in relazione a un'attività investigativa in corso.

Il sistema impiegato deve essere programmato in modo da operare al momento prefissato – ove tecnicamente possibile – la cancellazione automatica da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

Massimo 24 h	Massimo 7 gg.	Superiore a 7 gg.
È il termine di conservazione usuale. Sono fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si debba aderire a una specifica richiesta investigativa dell'Autorità giudiziaria o di polizia giudiziaria.	È ammesso un tempo più ampio di conservazione dei dati, che non può comunque superare la settimana, solo in alcuni specifici 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).	Un eventuale allungamento dei tempi di conservazione oltre la settimana 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 dall'Autorità giudiziaria o di polizia giudiziaria in relazione ad un'attività investigativa in corso.

TABELLA 1
TERMINI MASSIMI DI CONSERVAZIONE DEI DATI PERSONALI RACCOLTI ATTRAVERSO SISTEMI DI VIDEOSORVEGLIANZA

3.5 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".

Documentazione scritta delle scelte di trattamento dei dati

www.istockphoto.com

3.6 Diritti degli interessati

Rispetto dei diritti dei soggetti identificabili

"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 e di ottenere l'interruzione di un trattamento illecito, in specie quando non sono adottate idonee misure di sicurezza o il sistema è utilizzato da persone non debitamente autorizzate (art. 7 del Codice).

La risposta a una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti alla persona istante identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal Codice (art. 10, commi 3 s., del Codice). A tal fine può essere opportuno che la verifica dell'identità del richiedente avvenga mediante esibizione o allegazione di un documento di riconoscimento che evidenzi un'immagine riconoscibile dell'interessato".

3.7 Sanzioni

Sanzioni per il trattamento illecito dei dati

Il trattamento dei dati mediante videosorveglianza illecito oppure non corretto 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 s. del Codice).

Riepilogando

---

a) La videosorveglianza pone problemi relativi al trattamento dei dati personali.

b) Il trattamento dei dati personali mediante videosorveglianza deve innanzitutto rispondere alle norme del codice in materia di protezione dei dati personali.

c) L'impiego di sistemi di videosorveglianza deve inoltre essere conforme anche ad altre normative che disciplinano la materia: ad esempio, lo statuto dei lavoratori.

d) Il Garante per la protezione dei dati personali ha emanato nel 2004 un provvedimento generale nel quale sono riassunti i principi e gli adempimenti relativi al trattamento dei dati personali mediante videosorveglianza.

e) I principi relativi al trattamento dei dati personali mediante videosorveglianza sono:
- principio di liceità: il trattamento dei dati attraverso sistemi di videosorveglianza deve essere fondato su uno dei presupposti di liceità previsti dal Codice;
- principio di necessità: ciascun sistema informativo e il relativo programma informatico vanno 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, nonché in modo da cancellare periodicamente e automaticamente i dati eventualmente registrati;
- principio di proporzionalità: gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano attentamente valutate come insufficienti o inattuabili;
- principio di finalità: gli scopi perseguiti con il trattamento attuato mediante videosorveglianza devono essere determinati, espliciti e legittimi.

f) Gli adempimenti, che costituiscono sempre il presupposto per rendere lecito il trattamento dei dati personali mediante videosorveglianza, devono seguire alcune linee:
- va predisposta l'informativa: gli interessati devono essere informati che stanno per accedere o che si trovano in una zona videosorvegliata e dell'eventuale registrazione;
- i trattamenti di dati sensibili o giudiziari devono essere autorizzati preventivamente dal Garante;
- tutte le persone fisiche incaricate del trattamento devono essere designate per iscritto;
- i dati devono essere protetti da idonee e preventive misure di sicurezza, alcune misure c.d. minime sono obbligatorie anche sul piano penale;
- l'eventuale conservazione temporanea dei dati deve essere commisurata al grado di indispensabilità e per il solo tempo necessario – e predeterminato – a raggiungere la finalità perseguita;
- le ragioni delle scelte, relative al trattamento dei dati personali mediante videosorveglianza, devono essere adeguatamente documentate per iscritto.

g) Ulteriori adempimenti possono rendersi opportuni o necessari:
- è opportuno che si richieda al Garante una verifica preliminare delle scelte relative al trattamento dei sistemi di videosorveglianza, quando questi ultimi sono particolarmente invasivi della privacy;
- i trattamenti di dati a mezzo videosorveglianza devono essere notificati al Garante solo nei casi specificamente previsti dall'art. 37 del Codice.

h) Diritti degli interessati: deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al Codice.

i) Sanzioni per il trattamento illecito o non corretto:
- inutilizzabilità dei dati personali trattati;
- blocco o divieto del trattamento;
- sanzioni amministrative o penali.

Adempimenti sempre necessari	Adempimenti eventualmente necessari o opportuni
Informativa	Verifica preliminare del Garante delle scelte relative al trattamento dei sistemi di videosorveglianza quando questi ultimi sono particolarmente invasivi della privacy
Autorizzazione preventiva del Garante quando sono trattati dati sensibili o giudiziari	Nei casi specificamente previsti dall'art. 37 del Codice i trattamenti di dati a mezzo videosorveglianza devono essere notificati al Garante
Designazione per iscritto delle persone fisiche incaricate del trattamento	
Attuazione di misure idonee e preventive di sicurezza	
Cancellazione dei dati dopo l'eventuale e temporaneo periodo di conservazione	
Documentazione per iscritto delle ragioni delle scelte relative al trattamento dei dati personali	

TABELLA 2
ADEMPIMENTI NECESSARI PER RENDERE LECITO IL TRATTAMENTO DEI DATI PERSONALI MEDIANTE VIDEOSORVEGLIANZA

B. DALLA TEORIA ALLA PRATICA: LE PROCEDURE DA SEGUIRE IN ALCUNI CASI SPECIFICI

1. PREMESSA: LA VIDEOSORVEGLIANZA DA PARTE DI SOGGETTI PUBBLICI

Soggetti pubblici: il trattamento è lecito solo per funzioni istituzionali

Il Garante nel suo provvedimento generale del 2004 ha richiamato i presupposti per la liceità del trattamento dei dati personali mediante videosorveglianza effettuato da un soggetto pubblico.

1) "Un soggetto pubblico può effettuare attività di videosorveglianza solo e esclusivamente per svolgere funzioni istituzionali che deve individuare e esplicitare con esattezza e di cui sia realmente titolare in base all'ordinamento di riferimento (art. 18, comma 2, del Codice). 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 (art. 19, comma 2, del Codice)".

Esempio: l'illiceità è stata riscontrata con riguardo ad alcuni enti locali che hanno dichiarato di perseguire direttamente, in via amministrativa, finalità di prevenzione e accertamento dei reati che invece competono alle Autorità giudiziarie e alle Forze di polizia.

Soggetti pubblici: finalità di prevenzione e repressione di pericoli concreti e specifici

2) Quando il soggetto è realmente titolare di un compito attribuito dalla legge in materia di sicurezza pubblica o di accertamento, prevenzione e repressione di reati, per procedere a una videosorveglianza di soggetti identificabili deve ricorrere un'esigenza effettiva e proporzionata di prevenzione o repressione di pericoli concreti e specifici di lesione di un bene.

Esempio: non risulta lecito procedere, senza le necessarie e corrette valutazioni preliminari, ad una *videosorveglianza capillare di intere aree cittadine*, riprese integralmente e costantemente e senza adeguate esigenze.

Esempio: è vietato *il collegamento telematico tra più soggetti*, magari raccordati a un "centro" elettronico, che possa registrare un numero elevato di dati personali e ricostruire interi percorsi effettuati in un determinato arco di tempo.

Esempio: è priva di giustificazione l'installazione di impianti di videosorveglianza al solo fine di controllare il rispetto del *divieto di fumare o gettare mozziconi, di calpestare aiuole, di affiggere o di fotografare*, o di altri divieti relativi alle modalità nel depositare i sacchetti di immondizia entro gli appositi contenitori.

3) Le specifiche norme di legge o di regolamento e le funzioni legittimamente individuate dall'ente costituiscono l'ambito operativo entro il quale il trattamento dei dati si intende consentito. Come prescritto dal Codice, l'eventuale comunicazione a terzi è lecita solo se espressamente prevista da una norma di legge o di regolamento (art. 19, comma 3, del Codice).

4) Il Codice individua specifiche regole volte a consentire, in un quadro di garanzie, riprese audio-video a fini di documentazione dell'attività istituzionale di organi pubblici (artt. 20-22 e 65 del Codice).

5) Salvo i casi previsti per le professioni sanitarie e gli organismi sanitari, il soggetto pubblico non deve richiedere la manifestazione del consenso degli interessati (art. 18, comma 4, del Codice).

2. Controllo del traffico

Esempio: il Comune di "Isola che non c'è" decide di monitorare, attraverso sistemi di videosorveglianza, le zone nevralgiche del traffico cittadino al fine di effettuare l'analisi dei flussi dei veicoli e di agevolare la predisposizione di piani comunali relativi alla viabilità.

www.istockphoto.com

Gli adempimenti da rispettare

In una serie di occasioni – v., fra gli altri, i pareri 7 marzo 2000, Bollettino del n. 11/gennaio 2000, pag. 76; 7 marzo 2000, Bollettino del n. 11/gennaio 2000, pag. 73 – il Garante ha rilevato relativamente agli adempimenti, già illustrati nella parte A, che in particolare sono necessarie:

1) una limitazione delle modalità di ripresa delle immagini (memorizzazione, conservazione, angolo visuale delle telecamere e limitazione della possibilità di ingrandimento dell'immagine), anche al fine di assicurare il rispetto dei principi fondamentali fissati dal Codice, specie in ordine alla pertinenza e non eccedenza dei dati rispetto agli scopi perseguiti;

2) l'individuazione dei soggetti legittimati all'accesso, alla custodia e all'utilizzazione delle registrazioni anche all'interno dell'ente, escludendo dall'accesso le persone diverse dai responsabili e dagli incaricati. In proposito deve essere chiaramente esplicitato che l'utilizzo dei dati personali da parte del Comune nell'attività di videosorveglianza si colloca nella cornice normativa relativa allo svolgimento delle funzioni istituzionali e non è pertanto orientato alla raccolta e al trattamento di dati sensibili;

3) una puntuale verifica e disciplina per quanto riguarda l'eventuale messa a disposizione delle registrazioni in favore di altri soggetti pubblici;

4) l'indicazione del soggetto, o della struttura, cui il cittadino può rivolgersi per esercitare i propri diritti (art. 7 del Codice);

5) l'indicazione delle modalità dell'eventuale riutilizzazione dei supporti magnetici una volta cancellate le registrazioni;

6) la precisazione che ai fini dell'analisi dei flussi di traffico il trattamento è effettuato con modalità volta a salvaguardare l'anonimato, ma solo successivamente alla fase della raccolta, giacché le immagini registrate possono contenere dati di carattere personale.

Casi particolari: rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato

Il Comune di "Isola che non c'è" decide di limitare l'accesso di veicoli al centro storico. A questo scopo intende installare sistemi di videosorveglianza.

Sulla rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato il Garante ha osservato che "per gli aspetti

riguardanti [...] l'installazione e l'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato, è stata introdotta una recente disciplina che prevede tra l'altro, per i Comuni interessati, l'obbligo di munirsi di un'autorizzazione rilasciata dal Ministero dei lavori pubblici – Ispettorato generale per la circolazione e la sicurezza stradale (d.p.r. 22 giugno 1999, n. 250).

www.istockphoto.com

Tale regolamento prevede inoltre che gli impianti debbano essere utilizzati per raccogliere dati riguardanti il luogo, il tempo e l'identificazione dei veicoli che accedono al centro storico o alle zone a traffico limitato, rilevando immagini solamente in caso di infrazione.

Obbligo di autorizzazione per il monitoraggio degli accessi di veicoli ai centri storici e alle zone a traffico limitato

[...] Il citato regolamento prevede altresì che la documentazione con immagini sia utilizzata per le sole finalità di applicazione del regolamento medesimo e sia conservata solo per il periodo necessario alla contestazione dell'infrazione, all'applicazione della sanzione e alla definizione dell'eventuale contenzioso, salva l'eventuale ulteriore utilizzazione dei dati per esclusive finalità di polizia giudiziaria o di indagine penale".

Il Garante ha inoltre precisato che il d.p.r. 22 giugno 1999, n. 250 è applicabile unitamente alla disciplina del trattamento dei dati personali (oggi contenuta nel Codice).

Riepilogando

a) I Comuni possono fare uso di sistemi di videosorveglianza per il controllo del traffico, ma devono essere rispettati gli adempimenti illustrati nel provvedimento generale del Garante del 2004.

b) In particolare, occorre:
- limitare le modalità di ripresa delle immagini;
- individuare i soggetti legittimati all'accesso, alla custodia e all'utilizzazione delle registrazioni;
- verificare rigorosamente e disciplinare l'eventuale messa a disposizione delle registrazioni in favore di altri soggetti pubblici;
- indicare il soggetto, o la struttura, cui il cittadino può rivolgersi per esercitare i propri diritti;
- indicare le modalità dell'eventuale riutilizzazione dei supporti magnetici una volta cancellate le registrazioni;
- precisare che le immagini registrate possono contenere dati di carattere personale e che, successivamente alla fase della raccolta, il trattamento è effettuato con modalità volta a salvaguardare l'anonimato.

c) Per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato occorre adempiere non solo alle prescrizioni del codice in materia di trattamento dei dati personali, ma anche a quelle poste dal d.p.r. 22 giugno 1999, n. 250; in particolare, i Comuni devono munirsi dell'autorizzazione rilasciata dal Ministero dei lavori pubblici – Ispettorato generale per la circolazione e la sicurezza stradale.

Controllo del traffico	Rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato
Limitazione delle modalità di ripresa delle immagini	Idem
Individuazione dei soggetti legittimati all'accesso, alla custodia e all'utilizzazione delle registrazioni	Idem
Verifica rigorosa e disciplina dell'eventuale messa a disposizione delle registrazioni in favore di altri soggetti pubblici	Idem
Indicazione del soggetto o della struttura, cui il cittadino può rivolgersi per esercitare i propri diritti	Idem
Indicazione delle modalità dell'eventuale riutilizzazione dei supporti magnetici una volta cancellate le registrazioni	Idem
Precisazione del fatto che le immagini registrate possono contenere dati di carattere personale e che, successivamente alla fase della raccolta, il trattamento è effettuato con modalità volta a salvaguardare l'anonimato	Idem
	Ottenimento dell'autorizzazione rilasciata dal Ministero dei lavori pubblici – Ispettorato generale per la circolazione e la sicurezza stradale

TABELLA 3
ADEMPIMENTI SPECIFICI PER RENDERE LECITO IL TRATTAMENTO DEI DATI MEDIANTE VIDEOSORVEGLIANZA FINALIZZATO AL CONTROLLO DEL TRAFFICO URBANO DA PARTE DI UN COMUNE

3. Controllo di spazi pubblici

Esempio: il Comune di "Paese dei Balocchi" decide di varare un progetto di installazione di un sistema di tele-sorveglianza in alcune zone della città.

Adempimenti da rispettare

Devono essere rispettati gli adempimenti illustrati nella parte A con le specificazioni indicate al precedente paragrafo 2 di questa parte B.

Casi particolari: videocamere anticrimine sui mezzi di trasporto pubblico e alle fermate

Controllo degli spazi pubblici (autobus, fermate) solo per fini istituzionali

Il Comune di "Paese dei Balocchi", in accordo con il Prefetto e le Autorità di pubblica sicurezza, nel quadro di un'azione mirante a contenere il fenomeno della criminalità e a diminuire la pericolosità di ambiti cittadini particolarmente insicuri ha individuato come prioritario il settore del trasporto pubblico urbano, con particolare riguardo alla sicurezza dei viaggiatori su autobus e tram e alla prevenzione di reati e atti di vandalismo presso le fermate. A questo fine è stata ipotizzata la costruzione di un sistema di video-sorveglianza attraverso l'installazione, in via sperimentale, di telecamere su alcune linee di autobus e tram e presso alcune fermate.

Su questa tipologia di casi il Garante ha avuto occasione di pronunciarsi (v. il parere 23 marzo 1999, Bollettino del n. 8/marzo 1999, pag. 57; nonché il provvedimento generale del 2004 più volte richiamato).

www.istockphoto.com

Il Garante ha osservato preliminarmente che il Comune, nel quadro delle proprie funzioni di tutela e sviluppo del benessere della comunità locale, svolge le funzioni di polizia locale (art. 1, legge 7 marzo 1986 n. 65). In questo quadro l'ATM, che esercita il servizio pubblico di trasporto, potrebbe essere configurata come "responsabile" del

trattamento. Ciò anche in forza del particolare legame fra Comune e ATM che ha natura giuridica di azienda speciale ai sensi dell'art. 23 della legge n. 142 del 1990. In base al comma 5 del citato art. 23 spetta infatti all'ente locale, fra l'altro, approvare gli atti fondamentali e determinare finalità e indirizzi dell'azienda. Fra questi può quindi rientrare la tutela del patrimonio pubblico e il miglioramento della qualità del servizio di trasporto oltre alla salvaguardia della sicurezza degli utenti, da conseguirsi anche con le modalità tecnologicamente più avanzate, quali, ad esempio, i controlli video.

Nel merito il Garante ha stabilito che prima dell'attivazione del sistema di videosorveglianza devono essere opportunamente regolati i seguenti profili.

1) Vanno determinate con precisione la localizzazione delle telecamere e le modalità di ripresa in aderenza alle finalità che hanno suggerito l'installazione del sistema stesso, tenendo conto dei principi fondamentali fissati dalla disciplina del trattamento dei dati personali [oggi contenuta nel Codice], specie in ordine alla pertinenza e non eccedenza dei dati rispetto agli scopi perseguiti. Al riguardo vanno predisposte modalità di ripresa che permettano di cogliere in modo panoramico, per quanto tecnicamente possibile, l'interno delle vetture o l'ambito di fermata, evitando riprese particolareggiate tali da essere eccessivamente intrusive della riservatezza delle persone o da permettere la rilevazione di particolari non rilevanti (giornali letti, particolari fisici, ecc.).

2) Va poi evitato che le telecamere riprendano in modo stabile le postazioni di guida degli autisti. Al riguardo si ricordano, infatti, i precisi limiti posti all'installazione di impianti audiovisivi dall'art. 4 della legge 20 maggio 1970 n. 300 (c.d. statuto dei lavoratori). Va poi evidenziato che in nessun modo immagini visionate per finalità di polizia giudiziaria possono essere utilizzate per controlli, anche indiretti, sull'attività dei dipendenti ATM.

3) Occorre definire con precisione i soggetti legittimati a trattare i dati personali, individuando altresì con precisione gli incaricati del trattamento.

4) Inoltre, poiché la visione "in chiaro" delle immagini registrate è strettamente connessa alla commissione di atti criminosi e alla previa denuncia degli stessi all'Autorità di polizia, si ritiene che l'accesso ai computer della c.d. "stazione di lettura" centrale debba essere consentito mediante il sistema della "doppia chiave" congiunta (una in possesso del personale preposto ATM, una in possesso dell'Autorità di polizia). Più in generale vanno previste tutte le più idonee misure di sicurezza onde evitare dispersione dei dati, accessi non autorizzati, ecc.. In particolare, va costantemente garantita l'impossibilità di accesso diretto alle immagini registrate

presso i computer locali a bordo dei mezzi o presso le fermate; la costante e regolare distruzione delle immagini non oggetto di segnalazione; il rigoroso controllo di sicurezza sui dati registrati che, a seguito di denuncia, andranno esaminati dall'Autorità di polizia.

5) I titolari del trattamento devono poi provvedere a informare gli interessati. A questo proposito particolare attenzione andrà posta nel segnalare convenientemente agli utenti del servizio di trasporto urbano l'esistenza del sistema di videosorveglianza. Gli autobus e i tram dotati di telecamere devono pertanto portare apposite indicazioni o contrassegni che diano conto con immediatezza della presenza dell'impianto in esame, oltre a contenere all'interno della vettura un'informativa che riporti tutti i dati richiesti dall'art. 13 del Codice. Per quanto concerne poi le aree di fermata, nelle quali transitano o si soffermano anche persone che non utilizzano i mezzi pubblici, l'esistenza delle telecamere va opportunamente evidenziata, anche attraverso un'apposita segnaletica orizzontale che indichi con chiarezza le aree soggette a video-sorveglianza.

Casi particolari: deposito dei rifiuti

Il Comune di "Paese dei Balocchi" sottopone preliminarmente al Garante un progetto di videosorveglianza del deposito di rifiuti.

A proposito della videosorveglianza dei depositi di rifiuti il Garante ha osservato quanto segue (v., il provvedimento generale del 2004, nonché le indicazioni riguardanti la raccolta differenziata dei rifiuti del 14 luglio 2005, doc. web n. 1149822).

Monitoraggio del deposito rifiuti solo nelle aree abusive

"Il controllo video di aree abusivamente impiegate come discariche di materiali e di sostanze pericolose è lecito se risultano inefficaci o inattuabili altre misure".

www.istockphoto.com

"Il medesimo controllo non è invece lecito – e va effettuato in altra forma – se è volto ad accertare solo infrazioni amministrative rispetto a disposizioni concernenti modalità e orario di deposito dei rifiuti urbani".

Riepilogando

---

a) I Comuni possono fare uso di sistemi di videosorveglianza per il controllo di spazi pubblici, purché siano rispettati i principi e le prescrizioni illustrati nel provvedimento generale del Garante del 2004.

b) In particolare occorre ricordare che un soggetto pubblico può effettuare attività di videosorveglianza solo e esclusivamente per svolgere funzioni istituzionali che deve individuare e esplicitare con esattezza e di cui sia realmente titolare in base all'ordinamento di riferimento.

c) In ogni caso occorre rispettare i seguenti adempimenti che costituiscono sempre il presupposto per rendere lecito il trattamento dei dati personali mediante videosorveglianza:
- l'informativa;
- la richiesta al Garante di autorizzazione preventiva per i trattamenti di dati sensibili o giudiziari;
- la designazione per iscritto delle persone fisiche incaricate del trattamento;
- la protezione dei dati mediante idonee e preventive misure di sicurezza;
- la distruzione dei dati dopo un periodo, minimo e commisurato alla finalità perseguita con il trattamento, di conservazione;
- la documentazione per iscritto delle ragioni delle scelte, relative al trattamento dei dati personali.

d) Per ciò che concerne la videosorveglianza anticrimine sui mezzi di trasporto pubblico e alle fermate occorre in particolare:
- determinare con precisione la localizzazione delle telecamere e le modalità di ripresa in aderenza alle finalità che hanno suggerito l'installazione del sistema stesso, evitando riprese particolareggiate tali da essere eccessivamente intrusive della riservatezza delle persone;
- evitare che le telecamere riprendano in modo stabile le postazioni di guida degli autisti;
- far sì che l'accesso ai computer della c.d. "stazione di lettura" centrale debba essere consentito mediante il sistema della "doppia chiave" congiunta (una in possesso del personale preposto ATM, una in possesso dell'Autorità di polizia).

e) Per ciò che concerne la videosorveglianza del deposito dei rifiuti occorre ricordare:
- il controllo video è consentito solo per le aree abusivamente

impiegate come discariche di materiali e di sostanze pericolose e quando risultano inefficaci o inattuabili altre misure;
- il controllo non è invece lecito se è volto ad accertare solo infrazioni amministrative rispetto a disposizioni concernenti modalità e orario di deposito dei rifiuti urbani.

4. Rapporti di lavoro

Esempio: il Comune di "Paese delle Meraviglie" chiede se è lecito impiantare un sistema di videosorveglianza nei propri uffici. Il Comune in particolare chiede quali siano le implicazioni sul piano della privacy dei propri impiegati.

Adempimenti da rispettare

Il Garante nel provvedimento generale del 2004 ha osservato quanto segue a proposito della videosorvegliaza in ambienti di lavoro.

1) Nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa e ciò anche in caso di erogazione di servizi per via telematica mediante c.d. "web contact center".

2) Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è impiegata per esigenze organizzative e dei processi produttivi, ovvero è richiesta per la sicurezza del lavoro (art. 4 legge n. 300/1970; art. 2 d.lgs. n. 165/2001).

3) Queste garanzie vanno osservate sia all'interno degli edifici, sia in altri luoghi di prestazione di lavoro (ad esempio postazioni di guida sugli autobus).

4) È inammissibile l'installazione di sistemi di videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all'attività lavorativa (ad esempio bagni, spogliatoi, docce, armadietti e luoghi ricreativi).

5) 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 e altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull'attività giornalistica contenute nel Codice, fermi restando,

Videosorveglianza nei luoghi di lavoro nel rispetto dello statuto dei lavoratori

comunque, i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l'osservanza del codice deontologico per l'attività giornalistica e il diritto del lavoratore a tutelare la propria immagine opponendosi anche, per motivi legittimi, alla sua diffusione.

Riepilogando

a) Quando si intendono installare sistemi di videosorveglianza in luoghi di lavoro, come uffici pubblici o mezzi di trasporto, occorre rispettare non solo le previsioni del codice in materia di protezione dei dati personali, ma anche le norme dello statuto dei lavoratori (legge n. 300/1970).

b) In ogni caso è vietato il controllo a distanza dell'attività lavorativa.

c) Quando la videosorveglianza è necessaria per esigenze organizzative e dei processi produttivi, ovvero è richiesta per la sicurezza del lavoro, occorre rispettare le garanzie previste dallo statuto dei lavoratori.

d) È in ogni caso inammissibile l'installazione di sistemi di videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all'attività lavorativa (ad esempio bagni, spogliato, docce, armadietti e luoghi ricreativi).

e) Eventuali riprese televisive mirate a documentare attività od operazioni solo per scopi divulgativi o di comunicazione istituzionale o aziendale, che vedano coinvolto il personale dipendente, possono essere assimilate ai trattamenti temporanei finalizzati alla pubblicazione occasionale di articoli, saggi e altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull'attività giornalistica contenute nel Codice.

5. Ospedali e luoghi di cura

Esempio: l'Azienda Sanitaria Locale del Comune di "Isola che non c'è" chiede se è lecita l'installazione di un sistema di videosorveglianza all'interno delle proprie strutture ospedaliere.

Adempimenti da rispettare

Il Garante nel provvedimento generale del 2004 ha osservato quanto segue a proposito della videosorvegliaza riguardante ospedali e luoghi di cura.

www.istockphoto.com

Limiti stringenti alla videosorveglianza nelle strutture ospedaliere

1) L'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (ad esempio unità di rianimazione), stante la natura sensibile di molti dati che possono essere in tal modo raccolti, devono essere limitati ai casi di stretta indispensabilità e circoscrivendo le riprese solo a determinati locali e a precise fasce orarie; 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 delle doverose misure che il Codice prescrive per le strutture sanitarie (art. 83).

2) Il titolare deve garantire che possano accedere alle immagini solo i soggetti specificamente autorizzati (ad esempio personale medico e infermieristico) e che le stesse non possano essere visionate da estranei (ad esempio visitatori). Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di familiari di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (ad esempio rianimazione), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto.

3) Le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse, a pena di sanzione penale (artt. 22, comma 8, e 167 del Codice). Va assolutamente evitato il rischio di diffusione delle immagini di persone malate su monitor collocati in locali liberamente accessibili al pubblico.

4) Nei casi in cui l'impiego di un sistema di videosorveglianza all'interno di una struttura sanitaria non sia finalizzato alla cura del paziente, bensì solo a finalità amministrative o di sicurezza (quali, ad esempio, il controllo dell'edificio o di alcuni locali), e sia possibile che attraverso lo stesso siano

raccolte immagini idonee a rivelare lo stato di salute, il soggetto pubblico titolare deve menzionare tale trattamento nell'atto regolamentare sui dati sensibili da adottare in base al Codice (art. 20).

Riepilogando

a) La videosorveglianza in ospedali e luoghi di cura soggiace a limiti stringenti, stante la natura dei dati sensibili potenzialmente coinvolti.

b) L'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (ad esempio unità di rianimazione) devono essere limitati ai casi di stretta indispensabilità e circoscrivendo le riprese solo a determinati locali e a precise fasce orarie.

c) Devono essere adottati tutti gli ulteriori accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate, anche in attuazione delle doverose misure che il Codice prescrive per le strutture sanitarie (art. 83).

d) Il titolare deve garantire che possano accedere alle immagini solo i soggetti specificamente autorizzati.

e) Le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse, a pena di sanzione penale (artt. 22, comma 8, e 167 del Codice).

f) Nei casi in cui l'impiego di un sistema di videosorveglianza all'interno di una struttura sanitaria non sia finalizzato alla cura del paziente, bensì solo a finalità amministrative o di sicurezza e sia possibile che attraverso lo stesso siano raccolte immagini idonee a rivelare lo stato di salute, il soggetto pubblico titolare deve menzionare tale trattamento nell'atto regolamentare sui dati sensibili da adottare in base al Codice (art. 20).

6. ISTITUTI SCOLASTICI

Esempio: l'istituto scolastico di scuola media inferiore del Comune di "Paese dei Balocchi" chiede se è lecita l'installazione di un sistema di videosorveglianza all'interno e all'esterno delle proprie strutture.

Adempimenti da rispettare

Il Garante nel provvedimento generale del 2004 ha osservato quanto segue a proposito della videosorveglianza riguardante gli istituti scolastici.

1) 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) e tenere conto della delicatezza dell'eventuale trattamento di dati relativi a minori.

Monitoraggio degli istituti scolastici: diritto alla riservatezza dello studente e protezione per i minori

2) A tal fine, se può risultare ammissibile l'utilizzo di sistemi di videosorveglianza in casi di stretta indispensabilità, gli stessi devono essere circoscritti alle sole aree interessate e attivati negli orari di chiusura degli istituti, regolando rigorosamente l'eventuale accesso ai dati.

Esempio: casi di stretta indispensabilità possono essere rappresentati da atti vandalici ripetuti e protratti nel tempo.

3) Restano di competenza dell'Autorità giudiziaria o di polizia le iniziative intraprese a fini di tutela dell'ordine pubblico o di individuazione di autori di atti criminali.

Esempio: restano di competenza dell'Autorità giudiziaria o di polizia le iniziative riguardanti spacciatori di stupefacenti, adescatori, ecc.

Riepilogando

a) 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).

b) L'eventuale installazione di sistemi di videosorveglianza presso istituti scolastici deve tenere conto della delicatezza dell'eventuale trattamento di dati relativi a minori.

c) L'utilizzo di sistemi di videosorveglianza può risultare ammissibile in casi di stretta indispensabilità (ad esempio a causa del protrarsi di atti vandalici).

d) La videosorveglianza deve essere circoscritta alle sole aree interessate e attivata negli orari di chiusura degli istituti.

e) Deve essere regolato rigorosamente l'eventuale accesso ai dati.

f) Restano di competenza dell'Autorità giudiziaria o di polizia le iniziative intraprese a fini di tutela dell'ordine pubblico o di individuazione di autori di atti criminali.

7. Luoghi di culto e di sepoltura

Esempio: il cimitero del Comune di "Paese delle Meraviglie" chiede se è lecita l'installazione di un sistema di videosorveglianza all'interno e all'esterno delle proprie strutture.

Controllo dei luoghi di culto solo nel concreto rischio di atti vandalici

Adempimenti da rispettare

Il Garante nel provvedimento generale del 2004 ha osservato quanto segue a proposito della videosorveglianza riguardante luoghi di culto e di sepoltura.

1) L'installazione di sistemi di videosorveglianza presso chiese o altri luoghi di culto o di ritrovo di fedeli deve essere oggetto di elevate cautele, 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.

2) Al fine di garantire il rispetto dei luoghi di sepoltura, 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.

Riepilogando

a) L'installazione di sistemi di videosorveglianza presso chiese o altri luoghi di culto o di ritrovo di fedeli deve essere oggetto di elevate cautele, stante il carattere sensibile delle informazioni relative all'appartenenza ad una determinata confessione religiosa.

b) 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.

8. Installazione di collegamenti tra sistemi di videosorveglianza di soggetti pubblici (e/o privati) e Centrali operative di Forze di polizia nazionali

Esempio: il Comune di "Paese delle Meraviglie" intende installare un sistema di videosorveglianza per controllare il quartiere "Balocco" dove si concentra un'intensa attività di spaccio di sostanze stupefacenti e di prostituzione. Non disponendo di una propria Sala operativa, chiede di installare il proprio sistema presso la Sala operativa di una Forza di polizia nazionale.

Collegamento dei sistemi di videosorveglianza con le Forze di polizia

Adempimenti da rispettare

Fermo restando il rispetto di tutte le prescrizioni del Garante della privacy, la circolare del Direttore generale del Dipartimento della pubblica sicurezza del Ministero dell'Interno di data 8 febbraio 2005 (n. 558/A/421.2/70/456) fornisce alcune indicazioni.

1) I Comitati provinciali per l'ordine e la sicurezza pubblica devono essere coinvolti nella scelta delle aree da monitorare. In seno ai Comitati, inoltre, potranno essere esaminate le effettive esigenze e la concreta utilità degli apparati di telecontrollo.

2) La circolare dispone che i collegamenti con le Sale o Centrali operative siano necessariamente circoscritti. La diretta visualizzazione delle immagini rilevate dai sistemi in parola nelle Sale o Centrali operative potrà essere, quindi, mantenuta nei soli casi, rigorosamente limitati, di obiettivi "istituzionali" particolarmente sensibili, che fanno parte di una configurazione sistemica dei mezzi di allarme e di intervento a tutela dell'ordine e della sicurezza pubblica, o di obiettivi di interesse strategico per la sicurezza primaria.

3) Al di fuori dei casi circoscritti, potrà essere valutata una soluzione mediata, in forza della quale il flusso delle immagini prodotto dai sistemi giunga, a seconda degli obiettivi da vigilare e nel rispetto delle competenze istituzionali, presso gli Organi di polizia locale ovvero presso Istituti di vigilanza, in grado di garantire i servizi di

monitoraggio e il conseguente, eventuale allertamento della Sala o Centrale operativa delle Forze di polizia, nei casi in cui vengano riscontrati allarmi o anomalie.

4) Sotto il profilo tecnologico, occorre in entrambi i casi rispettare le indicazioni fornite dalla nota tecnica allegata alla circolare (vedi Allegato 1).

Riepilogando

---

a) L'installazione di sistemi di videosorveglianza che coinvolgono Sale o Centrali operative delle Forze di polizia nazionali deve essere concertata con il Comitato provinciale per l'ordine e la sicurezza pubblica.

b) La diretta visualizzazione delle immagini rilevate dai sistemi in parola nelle Sale o Centrali operative può essere ammessa nei casi, rigorosamente limitati, di obiettivi "istituzionali" particolarmente sensibili.

c) Fuori dei casi sopra esposti potrà essere valutata una soluzione mediata con allertamento della Sala o Centrale operativa delle Forze di polizia in caso di allarmi o anomalie.

d) Vanno in ogni caso rispettate le indicazioni contenute nella nota tecnica allegata alla circolare del Direttore generale del Dipartimento della pubblica sicurezza del Ministero dell'Interno di data 8 febbraio 2005 (n. 558/A/421.2/70/456).

C. ASPETTI TECNICI: INFORMAZIONI GENERALI

1. Determinazione delle finalità e proporzionalità con gli strumenti adottati

Consigli pratici prima dell'installazione del sistema di videosorveglianza

In un elenco dei principi da seguire in materia di videosorveglianza, i principi di proporzionalità e liceità emergono sicuramente come gli aspetti più rilevanti. Tali principi hanno un impatto diretto e significativo sulla scelta del sistema di videosorveglianza, sulle funzionalità da implementare, sulla progettazione di dettaglio.

Verifica della necessità effettiva di deterrenza

La prima e più ovvia verifica da fare è sulla necessità effettiva di dotarsi di un tale sistema. Di norma, gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. In particolare, qualora l'installazione sia finalizzata alla protezione di beni (anche in relazione ad atti di vandalismo), devono risultare inefficaci o non realizzabili altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. In altre parole, la videosorveglianza deve essere considerata come *extrema ratio*.

Qualora da una attenta analisi risulti evidente l'inefficienza/insufficienza di altri sistemi di deterrenza, il sistema di videosorveglianza può essere installato tenendo comunque conto dei suddetti principi. In particolare, si possono richiamare alcune note pratiche, di seguito riportate.

- Si dovrà evitare la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorre un'effettiva esigenza di deterrenza. Si tratterà, quindi, di scegliere la dislocazione delle telecamere e l'inquadratura in modo tale da limitare l'angolo visuale delle riprese alla registrazione delle sole immagini indispensabili per il raggiungimento delle finalità perseguite.

Limitazione delle riprese di spazi pubblici

Esempio: una videocamera installata all'ingresso di una casa plurifamiliare non deve permettere di vedere chi entra in quale appartamento.

- Si dovrà delimitare rigorosamente l'inquadratura in modo da evitare o ridurre al minimo indispensabile la ripresa di luoghi pubblici o aperti al pubblico.

Esempio: qualora sia di legittimo e effettivo interesse la ripresa di un accesso ad un edificio prospiciente una strada pubblica, la ripresa dovrà evitare per quanto possibile di inquadrare la zona antistante l'edificio, in modo tale da non rendere possibile l'identificazione delle persone che ivi si trovano.

Accuratezza nella scelta del grado di dettaglio necessario delle riprese

- Si dovrà determinare accuratamente il grado di dettaglio necessario. In particolare, occorre definire se sia sufficiente, ai fini della sicurezza, rilevare immagini che non rendano identificabili i singoli cittadini, anche tramite ingrandimenti, o se sia realmente essenziale ai fini prefissi raccogliere immagini dettagliate. Questo aspetto influenza la scelta della risoluzione spaziale e cromatica della telecamera utilizzata (che può essere superiore a quella visualizzata dall'eventuale monitor del sistema), nonché la determinazione dell'angolo visuale e dello zoom. È altresì critica la scelta di sistemi avanzati che forniscano movimenti di brandeggio e zoom automatici, dato che tali accorgimenti possono garantire livelli di dettaglio adattativi.

Esempio: un sistema installato all'ingresso di una banca dovrà necessariamente rendere riconoscibili i volti, in quanto indispensabili per le indagini in caso di rapina. Un apparato contapersone utilizzato per misurare il grado di affollamento di un ambiente (una stazione, una piazza, un autobus) non avrà invece necessità di rendere identificabili i singoli individui.

Sempre con riferimento ai principi di liceità e proporzionalità, vale la pena di citare due casi particolari, ma largamente diffusi.

- *Videosorveglianza per sicurezza individuale*
  Gli impianti di videosorveglianza installati a tutela della sicurezza individuale (ad esempio controllo dell'accesso alla propria abitazione) hanno vincoli molto meno stringenti, essendo il trattamento effettuato a fini personali. I soggetti privati possono installare telecamere senza il consenso di soggetti terzi interessati (peraltro non facilmente acquisibile), sulla base delle prescrizioni indicate dal Garante, a patto che chi intenda rilevare le immagini persegua un interesse legittimo, cioè la tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, prevenzione incendi, ecc.
  Sussistono in ogni caso due obblighi da rispettare:
  1) le riprese devono essere limitate agli spazi interni o immediatamente antistanti gli accessi, evitando forme di videosorveglianza su aree circostanti che potrebbero limitare la libertà altrui, e 2) le informazioni raccolte non devono essere comunicate o diffuse ad altri.

- *Videosorveglianza sui luoghi di lavoro*
  Sussiste il divieto di controllare a distanza i lavoratori. Questo implica ovviamente il divieto di monitorare aree non destinate ad attività lavorativa (ad esempio bagni, spogliatoi, docce,

armadietti, luoghi ricreativi), ma limita anche la possibilità di riprendere immagini nelle zone a rischio. Dal punto di vista del progetto di sistema, questo può implicare la necessità di mascherare alcune zone dell'immagine.

Esempio: una telecamera installata nell'area pubblica di un'agenzia bancaria può richiedere il mascheramento dell'area riservata agli operatori degli sportelli (Fig. 1).

Figura 1 - *Videosorveglianza di uno sportello bancario. Per preservare i diritti degli sportellisti è possibile mascherare alcune zone (nel caso sopra, in particolare, le zone riservate agli operatori) in ottemperanza alle normative sulla sorveglianza nei posti di lavoro. La selezione delle aree da mascherare è impostabile da sistema in fase di installazione (cferrieux.free.fr/rome/rome14.htm).*

Le garanzie di cui al punto precedente valgono in generale e non solo nel caso di sistemi installati all'interno di edifici. Ad esempio, i sistemi di monitoraggio di mezzi di trasporto urbani (autobus, metropolitane), che si stanno rapidamente diffondendo a seguito del fenomeno terrorismo, non dovranno riprendere in modo stabile la postazione di guida. Le immagini ottenute non potranno comunque essere utilizzate per controlli, anche indiretti, sull'attività lavorativa degli addetti. Anche in questo caso si può ricorrere al mascheramento dell'area.

Fanno eccezione i sistemi di videosorveglianza impiegati per esigenze organizzative e dei processi produttivi, e in particolare per la sicurezza del lavoro, dove comunque vanno osservate le garanzie previste in materia di lavoro.

Riepilogando

Prima di installare un sistema di videosorveglianza occorre valutare se è effettivamente indispensabile. Se si giunge a questa conclusione, la scelta del sistema deve essere estremamente accurata, in modo da:

1. riprendere solo le zone che sono effettivamente utili;

2. garantire che le riprese siano poi effettivamente utilizzabili per gli scopi che hanno portato alla determinazione di dotarsi di un sistema di videosorveglianza.

Particolare attenzione va fatta nel caso di sistemi che riprendano aree pubbliche o luoghi di lavoro.

2. Conservazione e utilizzo del materiale

Nel caso delle norme per la conservazione e l'utilizzo del materiale, i principi di finalità e proporzionalità sono quelli dominanti. Sarà in particolare necessario determinare quali dati rilevare (ad esempio il sistema potrebbe essere attivato solo in presenza di particolari eventi), se registrarli o meno e come proteggerli, che uso farne, se avvalersi di una rete di comunicazione per trasmetterli a distanza, se creare una banca dati locali utilizzando eventuali strumenti di indicizzazione, se sfruttare tecnologie di elaborazione immagine sofisticate (detezione movimento, riconoscimento, abbinamento con altre basi di dati quali archivi biometrici), se far funzionare il sistema in maniera *stand-alone* o interconnetterlo con altri gestiti dallo stesso titolare o da terzi.

Per analizzare in maggior dettaglio gli aspetti salienti, vengono qui raggruppati sotto tre voci: registrazione e trasmissione, utilizzo e conservazione delle immagini.

- Registrazione e trasmissione delle immagini: deve essere limitata ai casi e ai momenti di effettiva necessità.
  – *Quando registrare*: indifferentemente dal fatto che sia realizzata in analogico o digitale, la registrazione dei dati deve essere giustificata da effettiva esigenza. Ad esempio, non è opportuno creare una banca dati quando, per le finalità perseguite, sia sufficiente installare un sistema a circuito chiuso di sola visione delle immagini.

Raccolta delle immagini limitata alle effettive necessità

Esempio: un sistema di monitoraggio del flusso veicolare lungo una strada non avrà necessità di memorizzare le singole immagini, ma piuttosto dati medi statistici sul traffico. Il segnale video può quindi essere acquisito, elaborato per estrarne le informazioni utili e cancellato immediatamente dopo.

  – *Attivazione automatica*: per limitare al minimo la registrazione delle immagini, si possono anche utilizzare sistemi di attivazione automatica basata su eventi (ad esempio collegamento con rilevatori di movimento o di effrazione). In questo caso, la registrazione si limita al periodo in cui è in atto un effettivo pericolo. È in ogni caso opportuno dotarsi di sistemi programmabili per attivarsi solo nei momenti di

effettiva necessità (ad esempio in un esercizio commerciale durante le ore di chiusura).

Esempio: in un sistema di videosorveglianza ad uso domestico è possibile far partire la registrazione del video solo in presenza di un tentativo di effrazione rilevato da sensori installati su porte e finestre.

– *Archiviazione strutturata e basi dati*: particolarmente delicati sono i casi relativi a sistemi di videosorveglianza che prevedano una raccolta di immagini collegata e/o incrociata e/o confrontata con altri particolari dati personali quali dati biometrici, codici identificativi di carte elettroniche o dispositivi di identificazione della voce, indicizzazione delle immagini. In questi casi è indicata la richiesta preventiva al Garante, che può fornire elementi utili per la corretta progettazione del sistema.
– *Collegamento a centri remoti*: anche l'utilizzo di specifiche soluzioni quali la trasmissione ad appositi centri di allarmi e segnali, oppure l'adozione di interventi automatici per effetto di meccanismi o sistemi automatizzati d'allarme (chiusura accessi, afflusso di personale di vigilanza, ecc.) richiedono particolari cautele.

- Utilizzo delle immagini: l'utilizzo delle immagini deve essere limitato strettamente agli scopi legittimi per cui il sistema è stato installato.
  – *Finalità e diffusione dei dati*: i dati raccolti per la protezione delle persone e delle cose non possono essere utilizzati per altre finalità e non devono essere comunicati a terzi salvo nei casi previsti o consentiti dalla legge, ad esempio su richiesta dell'Autorità giudiziaria. Fanno eccezione le riprese effettuate sui luoghi di lavoro per documentare attività od operazioni solo a scopo divulgativo o di comunicazione istituzionale o aziendale e che vedano coinvolto il personale dipendente, fatto salvo il diritto del lavoratore a tutelare la propria immagine.

Utilizzo delle immagini limitato agli scopi prefissati

Esempio: il proprietario di un negozio che ha installato una videocamera per ragioni di sicurezza non può utilizzare le immagini per scopi di marketing, né può comunicarle o venderle a terzi (eccetto Autorità giudiziarie) per qualsivoglia scopo.

- Conservazione e misure di sicurezza: i trattamenti effettuati come la raccolta, la comunicazione, la consultazione immediata o differita oppure la conservazione delle immagini devono rispettare i principi generali della protezione dei dati.
  – *Sicurezza dei dati*: il responsabile della videosorveglianza deve adottare tutti i provvedimenti tecnici e organizzativi necessari per proteggere i dati personali contro qualsiasi trattamento illecito. Questo include la necessità di proteggere il sistema da accessi illeciti (conservazione in luogo sicuro chiuso a chiave), nonché di dotarsi di sistemi di password,

eventualmente multi-livello, o altri sistemi di autenticazione (ad esempio biometrici) per l'accesso ai dati.
– *Duplicazione delle immagini*: è da evitare per quanto possibile la duplicazione delle immagini registrate.
– *Informativa*: se le immagini riprese sono collegate ad un archivio di dati, l'obbligo di informazione deve includere l'indicazione dell'ente presso cui si può far valere il diritto di accesso.
– *Responsabili incaricati*: occorre nominare uno o più responsabili incaricati del trattamento dei dati. Il numero deve essere il più possibile ristretto, in particolare quando ci si avvale di collaborazioni esterne.
– *Documentazione*: negli impianti di videosorveglianza più complessi o di grossa estensione, è opportuno prevedere una documentazione, da produrre a cura del responsabile del sistema, che indichi le procedure di sicurezza e i relativi responsabili. Questo può essere utile in sede di visite ispettive o per gestire l'esercizio dei diritti dell'interessato o casi di contenzioso.

Conservazione delle immagini accurata e documentabile

Riepilogando

I dati raccolti sono dati sensibili che richiedono un trattamento attento. In particolare occorre:

1. limitare la raccolta di dati a quanto sia effettivamente necessario;

2. limitare per quanto possibile la trasmissione e la duplicazione dei dati;

3. conservare e proteggere i dati in maniera accurata e documentabile.

3. Il tempo di vita dei dati

In caso di registrazione, il periodo di conservazione delle immagini deve essere limitato. Di norma occorre dotarsi di sistemi in grado di cancellare ciclicamente i dati entro un periodo che va da poche ore al massimo di una giornata. I più recenti sistemi in commercio prevedono la possibilità di impostare questo parametro in fase di installazione (con un massimo dipendente dalle caratteristiche del sistema). Nei sistemi più antiquati la durata della registrazione era spesso vincolata dal supporto di memorizzazione (nastro magnetico).

Conservazione dei dati per il tempo strettamente necessario

Il periodo può essere esteso a qualche giorno, fino al massimo di una settimana in casi particolari, quali:

- Esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi.

Esempio: un esercizio che chiude nel fine settimana può avere necessità di conservare i dati dal venerdì sera fino al lunedì successivo.

- In ambienti particolarmente a rischio, una conservazione più lunga dei dati può essere richiesta per agevolare successive indagini.

Esempio: nel caso di rapina in una banca può essere opportuno analizzare il video dei giorni precedenti per identificare eventuali sopralluoghi da parte dei criminali.

Ulteriori allungamenti dei tempi di conservazione devono essere considerati come eccezionali e comunque collegati a necessità derivanti da eventi già accaduti o realmente incombenti, oppure alla necessità di custodire o consegnare una copia specificamente richiesta dall'Autorità giudiziaria o di polizia giudiziaria in relazione ad un'attività investigativa in corso.

Dal punto di vista tecnico, le specifiche precedenti richiedono un sistema con operatività programmabile, con la possibilità di mantenere i dati in corrispondenza di determinati eventi o richieste da parte dell'utente, nonché con la possibilità di operare, qualora richiesta, la cancellazione automatica da ogni supporto, anche mediante sovraregistrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

Da notare che, come ricordato in precedenza, i sistemi di videosorveglianza privati che provvedono al monitoraggio di luoghi non aperti al pubblico, godono di vincoli meno stringenti. In questo caso la registrazione può estendersi anche ad intervalli di tempo molto più lunghi qualora le esigenze dell'utente lo richiedano (ad esempio assenza per vacanze).

Riepilogando

Conservare i dati per il minor tempo possibile, in base alle finalità per cui il sistema è stato installato. Se l'applicazione lo permette, conviene non memorizzarli neppure temporaneamente.

4. Uso legale dei dati e marchiatura

Un aspetto importante di un sistema di videosorveglianza usato per la prevenzione di azioni criminali consiste nella possibilità di utilizzare i dati acquisiti a scopo di indagine o come prova in successive azioni giudiziarie.

I principali problemi che sorgono in questo contesto sono quelli legati alla esatta collocazione temporale dei dati, alla loro qualità e alla verifica di autenticità.

Temporizzazione delle immagini

- Temporizzazione: è importante che il sistema di registrazione sia in grado di marcare i dati con l'esatto momento in cui sono stati acquisiti (il cosiddetto "*time stamp*"). Nei vecchi sistemi VCR (analogici) tipicamente l'informazione temporale (ora e giorno) veniva sovraimpressa all'immagine (Fig. 2). Nei sistemi più recenti (digitali) l'informazione può essere memorizzata in forma numerica nell'archivio, con il vantaggio di non cancellare parti del video e poter essere utilizzata a scopo di indicizzazione e ricerca rapida. È importante che il sistema sia dotato di un meccanismo efficiente e preciso di marchiatura temporale e che l'orologio utilizzato sia correttamente sincronizzato (in particolare in sistemi multi-camera). I sistemi più sofisticati garantiscono la sincronizzazione dell'orologio interno con precisioni al di sotto del secondo.

Figura 2 - *Esempio di "time stamp" in un video analogico. Oltre alla data e all'ora alcuni sistemi possono indicare il numero della telecamera, codici identificativi e altre informazioni (http://www.hammondpolice.com/press200203.htm).*

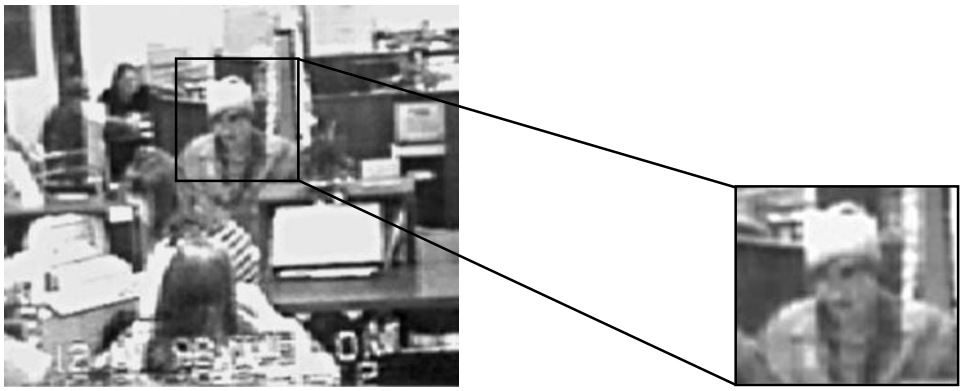
Qualità delle immagini

- Qualità del segnale: perché un video sia utilizzabile come prova, occorre che le immagini acquisite abbiano una qualità sufficiente per identificare in maniera accurata azioni e persone presenti nella scena ripresa.

Esempio: in caso di un furto in un appartamento, la telecamera dovrà fornire elementi per l'identificazione sicura del ladro e del fatto che abbia commesso l'azione per cui è incriminato.

Questo implica che il sistema abbia risoluzione sufficiente a rappresentare i tratti somatici degli individui nella scena, una qualità tale da non deteriorare le immagini (ad esempio immagine sfuocata, saturata, troppo scura, ecc.) e una inquadratura sufficientemente ampia da cogliere l'azione. Il sistema dovrà, quindi, avere caratteristiche adeguate allo scopo prefisso, essere installato e collaudato correttamente, e essere mantenuto in perfetta efficienza.

Figura 3 - *L'immagine è stata acquisita a risoluzione troppo bassa e con qualità scadente (probabilmente a causa delle caratteristiche scadenti del sensore e della scarsa illuminazione): questo la rende inutilizzabile ai fini del riconoscimento, anche qualora si effettui un ingrandimento del volto (http://www.louisville.edu/~gwover01/surveillance.html).*



- Autenticità dei dati: i più recenti sistemi di elaborazione di immagini rendono possibile contraffare le immagini in maniera quasi perfetta. Questo crea il problema di distinguere una immagine vera da un fotomontaggio.

Protezione del sistema e marchiatura delle immagini per l'autenticità

Esempio: in una sequenza che riprende una rapina in un negozio, l'esercente potrebbe ipoteticamente sostituire il volto del delinquente per causare l'arresto di un'altra persona.

Dal punto di vista legale esistono anche problemi più sottili quali il fatto che un segnale digitale può essere duplicato in maniera esatta, rendendo quindi ambiguo il concetto di "originale". Tecnicamente, il problema della autenticazione può essere risolto in due modi:

– *Protezione del sistema*: il sistema è realizzato in maniera tale da impedire l'accesso alle registrazioni da parte dell'utente, se non tramite un'autorità esterna. Questo accorgimento previene la manipolazione dei dati e garantisce l'autenticità degli stessi.

– *Marchiatura delle immagini*: più nota come *watermarking*, consiste nel sovrapporre all'immagine una sorta di firma digitale, che non altera la qualità dell'immagine, ma rende univocamente rilevabile la sorgente dell'immagine.
Il *watermark* può essere "permanente" (resistente agli attacchi), qualora lo si voglia usare per identificare con certezza la telecamera che ha generato il segnale, oppure "fragile" (facilmente deteriorabile) qualora lo scopo sia rilevare eventuali manipolazioni dei dati. Ovviamente, la marchiatura deve avvenire in modo automatico all'interno del sistema di acquisizione, e solo una autorità esterna deve disporre della chiave di decifrazione.

Figura 4 - *L'immagine in alto a sinistra è stata alterata cambiando lo sfondo e aggiungendo la tazza sul tavolo. Tramite il* watermark *entrambe le contraffazioni possono essere identificate (aree quadrettate nell'immagine in basso).*

Al momento non esiste uno standard per la marchiatura delle immagini, ma molti dei sistemi più avanzati implementano meccanismi di questo tipo.

Un ulteriore problema che può sorgere dipende dal fatto che il computer o comunque il sistema di acquisizione è una macchina, che come tale può funzionare in maniera non corretta. Perché i dati siano utilizzabili come prova occorre quindi una certificazione del fatto che il sistema che li ha acquisiti e registrati fosse funzionante e affidabile. Può essere anche utile

mantenere documentazione sulla manutenzione del sistema, sulle procedure operative seguite nella normale operazione e sul trattamento dei dati registrati a seguito di un evento. Parte di queste funzionalità possono essere fornite automaticamente dal sistema tramite i cosiddetti "*log file*", ovvero archivi dove vengono memorizzate in modo sincrono le operazioni svolte dal sistema.

Riepilogando

Per poter usare i dati raccolti dal sistema di videosorveglianza in un tribunale, occorre che questi siano "certificabili", ovvero:

1. che si possa identificarne la provenienza;
2. che si possa identificare l'istante in cui sono stati acquisiti;
3. che la qualità sia sufficiente a riconoscere cose, persone o azioni;
4. che si possa verificare che non siano stati alterati o manomessi.

Le moderne tecnologie di marchiatura e criptaggio, unite a misure di sicurezza sull'accesso fisico al sistema, possono garantire il rispetto di queste condizioni.

D. FREQUENTLY ASKED QUESTION

	DOMANDA	*RISPOSTA*
1	Esiste una regolamentazione organica dell'attività di videosorveglianza?	No. Esistono varie normative che disciplinano diversi profili della videosorveglianza. Tra le più rilevanti vi è il d.lgs. 30 giugno 2003, n. 196, codice in materia di protezione dei dati personali, il quale è applicabile al trattamento dei dati personali effettuato mediante videosorveglianza.
2	Il codice in materia di protezione dei dati personali contiene una disciplina specifica della videosorveglianza?	L'art. 134 del Codice è l'unico specificatamente dedicato alla materia. Esso prevede l'emanazione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini. Tale codice deontologico è ancora in fase di elaborazione.
3	Vi sono interpretazioni delle norme del Codice applicabili alla videosorveglianza?	Sì. Il Codice ha trovato in numerosi provvedimenti – decisioni su ricorsi, contestazioni di violazioni amministrative, pareri e provvedimenti generali – del Garante molte applicazioni alla materia della videosorveglianza. Le interpretazioni del Garante per la Protezione dei Dati Personali sono oggi riassunte nel provvedimento generale del 29 aprile 2004, reperibile sul sito Web del Garante www.garanteprivacy.it
4	Quali sono i principali adempimenti che occorre rispettare per rendere lecito il trattamento dei dati personali mediante sistemi di videosorveglianza?	*a)* Gli interessati devono essere informati che stanno per accedere o che si trovano in una zona videosorvegliata e dell'eventuale registrazione. *b)* I trattamenti di dati sensibili o giudiziari devono essere autorizzati preventivamente dal Garante. *c)* Tutte le persone fisiche incaricate del trattamento devono essere designate per iscritto. *d)* I dati devono essere protetti da idonee e preventive misure di sicurezza, alcune misure c.d. minime sono obbligatorie anche sul piano penale. *e)* L'eventuale conservazione temporanea dei dati deve essere commisurata al grado di indispensabilità e per il solo tempo necessario – e predeterminato – a raggiungere la finalità perseguita. *f)* Le ragioni delle scelte, relative al trattamento dei dati personali mediante videosorveglianza, devono essere adeguatamente documentate per iscritto.
5	Un soggetto pubblico deve chiedere il consenso all'interessato per poter trattare i suoi dati personali mediante videosorveglianza?	Generalmente no. Salvo i casi previsti per le professioni sanitarie e gli organismi sanitari, il soggetto pubblico non deve richiedere la manifestazione del consenso degli interessati.
6	Un Comune può fare uso di sistemi di videosorveglianza per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato?	Sì, ma deve rispettare alcune prescrizioni specifiche. Oltre agli adempimenti indicati nel provvedimento generale del Garante sulla videosorveglianza del 2004, il Comune deve munirsi di un'autorizzazione rilasciata dal Ministero dei lavori pubblici – Ispettorato generale per la circolazione e la sicurezza stradale, secondo quanto disposto dal d.p.r. 22 giugno 1999, n. 250.

	DOMANDA	*RISPOSTA*
7	Un Comune può fare uso di sistemi di videosorveglianza sui mezzi di trasporto pubblico e alle fermate in funzione anticrimine?	Sì, ma deve rispettare le prescrizioni specifiche indicate nel provvedimento generale del Garante sulla videosorveglianza del 2004. Occorre innanzitutto tenere presente che un soggetto pubblico può effettuare attività di videosorveglianza solo e esclusivamente per svolgere funzioni istituzionali che deve individuare e esplicitare con esattezza e di cui sia realmente titolare in base all'ordinamento di riferimento. Ciò detto, il Comune, nel quadro delle proprie funzioni di tutela e sviluppo del benessere della comunità locale, svolge le funzioni di polizia locale (art. 1, legge 7 marzo 1986 n. 65). In questo quadro l'ATM, che esercita il servizio pubblico di trasporto, potrebbe essere configurata come "responsabile" del trattamento. Con queste premesse, è possibile utilizzare la videosorveglianza sui mezzi di trasporto pubblico e alle fermate. Tuttavia, prima di procedere all'attivazione dei sistemi di videosorveglianza occorre predisporre tutte le cautele indicate nel provvedimento generale del Garante sulla videosorveglianza del 2004.
8	Un Comune può fare uso di sistemi di videosorveglianza per accertare le infrazioni amministrative relative a disposizioni concernenti modalità e orario di deposito dei rifiuti urbani?	No. Qualora risultino inefficaci o inattuabili altre misure, è lecito solo il controllo video di aree abusivamente impiegate come discariche di materiali e di sostanze pericolose.
9	Occorre adoperare particolari cautele quando si fa uso di un sistema di videosorveglianza in aree dove possono essere ripresi lavoratori dipendenti?	Sì. Posto che in ogni caso è vietato il controllo a distanza dell'attività lavorativa, quando la videosorveglianza è impiegata per esigenze organizzative e dei processi produttivi, ovvero è richiesta per la sicurezza del lavoro, occorre rispettare sia le norme del codice in materia di protezione dei dati personali, sia le garanzie previste dalla l. n. 300 del 1970, c.d. statuto dei lavoratori.
10	Occorre adoperare particolari cautele quando si fa uso di un sistema di videosorveglianza in ospedali e luoghi di cura?	Sì. La videosorveglianza in ospedali e luoghi di cura soggiace a limiti stringenti, stante la natura dei dati sensibili potenzialmente coinvolti. In particolare, la videosorveglianza deve essere limitata ai casi di stretta indispensabilità e circoscrivendo le riprese solo a determinati locali e a precise fasce orarie; il titolare del trattamento dei dati deve garantire che possano accedere alle immagini solo i soggetti specificamente autorizzati; le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse.
11	Occorre adoperare particolari cautele quando si fa uso di un sistema di videosorveglianza in istituti scolastici?	Sì. Soprattutto quando si tratta di istituti scolastici per minori. In particolare, la videosorveglianza deve essere circoscritta alle sole aree interessate e attivata negli orari di chiusura degli istituti; deve essere regolato rigorosamente l'eventuale accesso ai dati.
12	Occorre adoperare particolari cautele quando si fa uso di un sistema di videosorveglianza in luoghi di culto o sepoltura?	Sì. I dati relativi alle proprie convinzioni religiose sono dati sensibili e, perciò, soggetti ad una tutela rafforzata. L'installazione di sistemi di videosorveglianza presso chiese o altri luoghi di culto o di ritrovo di fedeli deve essere oggetto di elevate cautele.

E. GLOSSARIO

Brandeggio: movimentazione della telecamera (rotazione lungo i tre assi principali e eventuale traslazione tramite binari).

Biometrico: basato sulla misurazione di determinate caratteristiche del corpo umano, utili alla identificazione personale (ad esempio impronte digitali, iride, retina, tratti somatici).

Chiave di decifrazione: nella crittografia, la chiave di decifrazione indica la sequenza (tipicamente di numeri o lettere) che consente di operare la "crittanalisi", ovvero la ricostruzione del messaggio occultato.

Codice: d.lgs. 30 giugno 2003, codice in materia di protezione dei dati personali.

Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Crittografia: la crittografia tratta delle "scritture segrete", ovvero i metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile a persone non autorizzate.

Dati giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u), del d.p.r. 14 novembre 2002, n. 313, 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 artt. 60 e 61 del codice di procedura penale.

Dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato.

Dati sensibili: i dati personali idonei a rivelare l'origine razziale e 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.

Dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

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.

Definizione cromatica: capacità di uno strumento di rendere in maniera accurata la luminosità e la tinta di un oggetto osservato.

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Garante: Garante per la Protezione dei Dati Personali.

Indicizzazione: ordinamento in base a caratteristiche dei dati, tipicamente utilizzata per accedere più rapidamente alle informazioni in una base dati.

Incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Log file: è un file che viene generato automaticamente da un sistema, in cui vengono registrati tutti i dettagli sulla operatività del sistema stesso (funzioni eseguite, tentativi di accesso, allarmi, ecc.).

Misure di sicurezza: le misure di sicurezza imposte dall'art. 31 del Codice a chi tratta dati personali al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Misure minime: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'art. 31.

Notificazione al Garante: obbligo di notificare alcuni specifici trattamenti di dati personali previsti dall'art. 37 del Codice (come, ad esempio, i dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica).

Password: la password (parola chiave) è una forma di autenticazione che usa una stringa alfanumerica per controllare l'accesso a una risorsa. Il meccanismo di protezione è basato sulla segretezza della parola, che deve rimanere sconosciuta a coloro ai quali l'accesso non è garantito.

Password multi-livello: un sistema di password multi-livello può consentire un accesso gerarchico all'informazione. Ad esempio,

il proprietario di un sistema di videosorveglianza può avere una password che gli dà diritto alla sola visualizzazione dei dati, un'autorità esterna (ad esempio polizia) può essere dotata di una password che ne consente anche la duplicazione o modifica.

Responsabile: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

Risoluzione spaziale: capacità di uno strumento di distinguere e separare fra loro dettagli morfologici di un oggetto osservato. A un'alta risoluzione corrisponde una maggiore nitidezza dell'immagine.

Time-stamp: annotazione dei dati che indica la data e ora di un'azione e l'identità della persona o del sistema che ha generato e annotato i dati.

Titolare: 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.

Trattamento: qualunque operazione o complesso di 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 dati.

Verifica preliminare del Garante: adempimento che si rende opportuno al fine di verificare che il trattamento dei dati personali mediante sistemi di videosorveglianza particolarmente invasivi sia lecito e corretto.

Watermarking: il watermarking è una tecnica di cifratura che inserisce un segnale "trasparente" all'interno di un documento (testo, suono, immagine), tale da contenere informazioni sulla proprietà del documento o sulla sorgente che lo ha generato.

Watermark permanente: il watermark è permanente se è progettato per resistere a possibili "attacchi" (tentativi di rimozione o alterazione tramite manipolazione del documento ospite).

Watermark fragile: il watermark è fragile se viene facilmente alterato nel caso di manipolazione del documento ospite.

F. RIFERIMENTI ESSENZIALI

1. NORMATIVA

Circolare del Direttore generale del Dipartimento della pubblica sicurezza del Ministero dell'Interno di data 8 febbraio 2005 (n. 558/A/421.2/70/456).

Convenzione del Consiglio d'Europa n. 108/1981 del 28 gennaio 1981, sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale.

Direttiva del Parlamento Europeo e del Consiglio n. 95/46/CE del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Direttiva del Parlamento Europeo e del Consiglio n. 2002/58/CE del 12 luglio 2002, relativa alla vita privata e alle comunicazioni elettroniche.

d.lgs. 30 giugno 2003, n. 196, codice in materia di protezione dei dati personali.

l. 20 maggio 1970, n. 300, norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale nei luoghi di lavoro e norme sul collocamento.

d.m. del 6 giugno 2005, modifiche e integrazioni al decreto ministeriale 18 marzo 1996, recante norme di sicurezza per la costruzione e l'esercizio degli impianti sportivi.

d.lgs. 4 febbraio 2000, n. 45, attuazione della direttiva 98/18/CE relativa alle disposizioni e alle norme di sicurezza per le navi da passeggeri adibite a viaggi nazionali.

d.l. 24 febbraio 2003, n. 28, disposizioni urgenti per contrastare i fenomeni di violenza in occasione di competizioni sportive, convertito, con modificazioni, dalla l. 24 aprile 2003, n. 88.

d.p.r. 22 giugno 1999, n. 250, regolamento recante norme per l'autorizzazione all'installazione e all'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato, a norma dell'art. 7, comma 133-bis, della legge 15 maggio 1997, n. 127.

d.l. 14 novembre 1992, n. 433, misure urgenti per il funzionamento dei musei statali, convertito, con modificazioni, dalla legge 14 gennaio 1993, n. 4.

2. Provvedimenti del Garante per la Protezione dei Dati Personali

2.2 Provvedimenti generali

Provvedimento generale sulla videosorveglianza, 29 aprile 2004 [doc. web n. 1003482].

Provvedimento generale "Il decalogo delle regole per non violare la privacy", 29 novembre 2000 [doc. web n. 31019].

2.3 Altri provvedimenti

Decisione su ricorso, 19 dicembre 2001, Bollettino del n. 23/ottobre 2001, pag. 40 [doc. web n. 40085], diritto di accesso – Accesso ai dati acquisiti mediante un impianto di videosorveglianza.

28 settembre 2001 [doc. web n. 39704], videosorveglianza e dati biometrici – Rilevazioni biometriche presso istituti di credito.

Provvedimento, 14 giugno 2001 [doc. web n. 41782], videosorveglianza – Web-cam su spiagge.

7 marzo 2001 [doc. web n. 30947], videosorveglianza – Raccolta di impronte digitali associate ad immagini per l'accesso a banche.

Decisione su ricorso, 28 febbraio 2001, Bollettino del n. 17/febbraio 2001, pag. 35 [doc. web n. 40181], videosorveglianza – Videosorveglianza e rilevazione di impronte digitali all'ingresso di banche.

Parere – 7 marzo 2000, Bollettino del n. 11/gennaio 2000, pag. 73 [doc. web n. 40041], videosorveglianza – Città di Portici – Impianto di telecontrollo e videosorveglianza.

19 novembre 1999 [doc. web n. 42058], videosorveglianza e biometria – Trattamento dati personali mediante utilizzo di impronte digitali.

Parere – 23 marzo 1999, Bollettino del n. 8/marzo 1999, pag. 57 [doc. web n. 40899], videosorveglianza – Città di Torino – Videosorveglianza sui mezzi di trasporto pubblico urbano.

Parere – 28 maggio 1998, Bollettino del n. 4/marzo 1998, pag. 74 [doc. web n. 1002044], videosorveglianza – Installazione di alcune telecamere da parte di un Comune.

Parere – 17 dicembre 1997, Bollettino del n. 2/agosto 1997, pag. 57 [doc. web n. 39849], videosorveglianza – Installazione da

parte del Comune di Milano di alcune telecamere in luogo pubblico.

3. Altra documentazione

Gruppo di lavoro ex Articolo 29 Direttiva 95/46/CE: *Documento di lavoro – Sorveglianza delle comunicazioni elettroniche sul luogo di lavoro*, 25 novembre 2002.

Consiglio d'Europa, *Rapporto contenente le linee guida per la protezione delle persone con riguardo alla raccolta e al trattamento di dati per mezzo della videosorveglianza*, 20-23 maggio 2003.

Indagine esplorativa – *La videosorveglianza esterna visibile: una panoramica su quattro città*, giugno 2000.

APPENDICE

1. VIDEOSORVEGLIANZA – PROVVEDIMENTO GENERALE 29 APRILE 2004

SOMMARIO

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti, e del dott. Giovanni Buttarelli, segretario generale.
Visti gli atti d'ufficio e le osservazioni formulate ai sensi dell'art. 15 del regolamento n. 1/2000;

Relatore il prof. Gaetano Rasi;

RILEVATO

1. PREMESSA

Il Garante ritiene opportuno aggiornare e integrare il provvedimento del 29 novembre 2000 (c.d. "decalogo" pubblicato sul Bollettino del Garante n. 14/15, p. 28), anche per conformare i trattamenti di dati personali mediante videosorveglianza al Codice entrato in vigore il 1° gennaio 2004 e ad altre disposizioni vigenti (art. 154, comma 1, lett. c), d.lgs. 30 giugno 2003, n. 196, recante il codice in materia di protezione dei dati personali) che hanno rafforzato le garanzie per i cittadini. Per altro verso va evidenziato che nel triennio di applicazione del predetto provvedimento sono stati sottoposti all'esame dell'Autorità numerosi casi, 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 dei dati.

Con riferimento alle menzionate garanzie, il presente provvedimento (paragrafi 2 e 3) richiama taluni principi e illustra le prescrizioni generali relative a tutti i sistemi di videosorveglianza; nei paragrafi 4, 5 e 6 vengono invece individuate prescrizioni riguardanti specifici trattamenti di dati.
Ovviamente, per casi particolari l'Autorità si riserva di intervenire di volta in volta con atti ad hoc.

Le prescrizioni del presente provvedimento hanno come presupposto il rispetto dei diritti e delle libertà fondamentali dei cittadini e della dignità delle persone con particolare riferimento alla riservatezza, all'identità e alla protezione dei dati personali (art. 2, comma 1, del Codice).

Il Garante ha posto doverosa attenzione al nuovo diritto alla protezione dei dati personali (art. 1 del Codice) consapevole che un'idonea tutela dei diritti dei singoli, oggetto del bilanciamento effettuato con il presente provvedimento, non pregiudica l'adozione di misure efficaci per garantire la sicurezza dei cittadini e l'accertamento degli illeciti.

Si è avuto riguardo pertanto anche alla libertà di circolazione nei luoghi pubblici o aperti al pubblico. In tali ambiti, non si possono privare gli interessati del diritto di circolare senza subire ingerenze incompatibili con una libera società democratica (art. 8 conv. europea diritti dell'uomo

ratificata con l. n. 848/1955), derivanti da rilevazioni invadenti e oppressive riguardanti presenze, tracce di passaggi e spostamenti, facilitate dalla crescente interazione dei sistemi via Internet e Intranet.

Il Garante si è infine ispirato alle indicazioni espresse in varie sedi internazionali e comunitarie: in particolare alle linee-guida del Consiglio d'Europa del 20-23 maggio 2003 (v. Relazioni annuali del Garante per il 2002 e per il 2003, in www.garanteprivacy.it), nonché agli indirizzi formulati dalle autorità europee di protezione dei dati riunite nel Gruppo istituito dalla direttiva n. 95/46/CE (11 febbraio 2004, n. 4/2004, in Relaz. annuale 2003).

2. Principi Generali

2.1 Principio di liceità

Il trattamento dei dati attraverso sistemi di videosorveglianza è possibile solo se è fondato su uno dei presupposti di liceità che il Codice prevede espressamente per gli organi pubblici da un lato (svolgimento di funzioni istituzionali: artt. 18-22) e, dall'altro, per soggetti privati e enti pubblici economici (adempimento ad un obbligo di legge, provvedimento del Garante di c.d. "bilanciamento di interessi" o consenso libero e espresso: artt. 23-27). 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.

La videosorveglianza deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati, di quanto prescritto da altre disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi.

Vanno richiamate al riguardo le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela (toilette, stanze d'albergo, cabine, spogliatoi, ecc.). Vanno tenute presenti, inoltre, le norme riguardanti la tutela dei lavoratori, con particolare riferimento alla legge 300/1970 (statuto dei lavoratori).

Specifici limiti possono derivare da altre speciali disposizioni di legge o di regolamento che prevedono o ipotizzano la possibilità di installare apparecchiature di ripresa locale, aerea o satellitare (d.l. 24 febbraio 2003, n. 28, convertito, con modificazioni, dalla legge 24 aprile 2003, n. 88), disposizioni che, quando sono trattati dati relativi a persone identificate o identificabili, vanno applicate nel rispetto dei principi affermati dal Codice, in tema per esempio di sicurezza presso stadi e impianti sportivi, oppure musei, biblioteche statali e archivi di Stato (d.l. 14 novembre 1992, n. 433, convertito, con modificazioni, dalla legge 14 gennaio 1993, n. 4) e, ancora, relativi a impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali (d.lgs. 4 febbraio 2000, n. 45).

Appare inoltre evidente la necessità del rispetto delle norme del codice penale che vietano le intercettazioni di comunicazioni e conversazioni.

2.2. Principio di necessità

Poiché l'installazione di un sistema di videosorveglianza comporta in sostanza l'introduzione di un vincolo per il cittadino, ovvero di una limitazione e comunque di un condizionamento, va applicato il principio di necessità e, quindi, va escluso ogni uso superfluo e evitati eccessi e ridondanze.

Ciascun sistema informativo e il relativo programma informatico vanno 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 (ad esempio programma configurato in modo da consentire, per monitorare il traffico, solo riprese generali che escludano la possibilità di ingrandire le immagini). Il software va configurato anche in modo da cancellare periodicamente e automaticamente i dati eventualmente registrati.

Se non è osservato il principio di necessità le installazioni delle apparecchiature e l'attività di videosorveglianza non sono lecite (artt. 3 e 11, comma 1, lett. a), del Codice).

2.3. Principio di proporzionalità

Nel commisurare la necessità di un sistema al grado di rischio presente in concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorre un'effettiva esigenza di deterrenza, come quando, ad esempio, le telecamere vengono installate solo per meri fini di apparenza o di "prestigio".

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.

Non va adottata la scelta semplicemente meno costosa, o meno complicata, o di più rapida attuazione, che potrebbe non tener conto dell'impatto sui diritti degli altri cittadini o di chi abbia diversi legittimi interessi.

Non risulta di regola giustificata un'attività di sorveglianza rivolta non al controllo di eventi, situazioni e avvenimenti, ma a fini promozionali-turistici o pubblicitari, attraverso web cam o cameras-on-line che rendano identificabili i soggetti ripresi.
Anche l'installazione meramente dimostrativa o artefatta di telecamere non funzionanti o per finzione, anche se non comporta trattamento di dati personali, può determinare forme di condizionamento nei movimenti e nei comportamenti delle persone in luoghi pubblici e privati e pertanto può essere legittimamente oggetto di contestazione.

La videosorveglianza è, quindi, lecita solo se è rispettato il c.d. principio di proporzionalità, sia nella scelta se e quali apparecchiature di ripresa installare, sia nelle varie fasi del trattamento (art. 11, comma 1, lett. d), del Codice).

Il principio di proporzionalità consente, ovviamente, margini di libertà nella valutazione da parte del titolare del trattamento, ma non comporta scelte del tutto discrezionali e insindacabili.

Il titolare del trattamento, prima di installare un impianto di videosorveglianza, deve valutare, obiettivamente e con un approccio selettivo, se l'utilizzazione ipotizzata sia in concreto realmente proporzionata agli scopi prefissi e legittimamente perseguibili.

Si evita così un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli altri interessati.

Come si è detto, la proporzionalità va valutata in ogni fase o modalità del trattamento, per esempio quando si deve stabilire:

- se sia sufficiente, ai fini della sicurezza, rilevare immagini che non rendono identificabili i singoli cittadini, anche tramite ingrandimenti;
- se sia realmente essenziale ai fini prefissi raccogliere immagini dettagliate;
- la dislocazione, l'angolo visuale, l'uso di zoom automatici e le tipologie – fisse o mobili – delle apparecchiature;
- quali dati rilevare, se registrarli o meno, se avvalersi di una rete di comunicazione o creare una banca dati, indicizzarla, utilizzare funzioni di fermo-immagine o tecnologie digitali, abbinare altre informazioni o interconnettere il sistema con altri gestiti dallo stesso titolare o da terzi;
- la durata dell'eventuale conservazione (che, comunque, deve essere sempre temporanea).

In applicazione del predetto principio va altresì delimitata rigorosamente:

- anche presso luoghi pubblici o aperti al pubblico, quando sia di legittimo e effettivo interesse per particolari finalità, la ripresa di luoghi privati o di accessi a edifici;
- l'utilizzazione di specifiche soluzioni quali il collegamento ad appositi "centri" cui inviare segnali di allarme sonoro o visivo, oppure l'adozione di interventi automatici per effetto di meccanismi o sistemi automatizzati d'allarme (chiusura accessi, afflusso di personale di vigilanza, ecc.), tenendo anche conto che in caso di trattamenti volti a definire profili o personalità degli interessati il Codice prevede ulteriori garanzie (art. 14, comma 1, del Codice);
- l'eventuale duplicazione delle immagini registrate;

- la creazione di una banca dati quando, per le finalità perseguite, è sufficiente installare un sistema a circuito chiuso di sola visione delle immagini, senza registrazione (ad esempio per il monitoraggio del traffico o per il controllo del flusso ad uno sportello pubblico).

2.4. Principio di finalità

Gli scopi perseguiti devono essere determinati, espliciti e legittimi (art. 11, comma 1, lett. b), del Codice). Ciò comporta che il titolare possa perseguire solo finalità di sua pertinenza.

Si è invece constatato che taluni soggetti pubblici e privati si propongono abusivamente, quale scopo della videosorveglianza, finalità di sicurezza pubblica, prevenzione o accertamento dei reati che invece competono solo ad Organi giudiziari o di polizia giudiziaria oppure a Forze armate o di polizia.

Sono invece diversi i casi in cui i sistemi di videosorveglianza sono in realtà introdotti 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.

In ogni caso, possono essere perseguite solo finalità determinate e rese trasparenti, ossia direttamente conoscibili attraverso adeguate 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 (art. 11, comma 1, lett. b), del Codice). Le finalità così individuate devono essere correttamente riportate nell'informativa.

3. Adempimenti

3.1. Informativa

Gli interessati devono essere informati che stanno per accedere o che si trovano in una zona videosorvegliata e dell'eventuale registrazione; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (concerti, manifestazioni sportive) o di attività pubblicitarie (attraverso web cam).

L'informativa deve fornire gli elementi previsti dal Codice (art. 13) anche con formule sintetiche, ma chiare e senza ambiguità.

Tuttavia il Garante ha individuato ai sensi dell'art. 13, comma 3, del Codice un modello semplificato di informativa "minima", riportato in fac-simile in allegato al presente provvedimento (cfr. pag. 20) e che può essere utilizzato in particolare in aree esterne, fuori dei casi di verifica

preliminare indicati nel punto successivo. Il modello è ovviamente adattabile a varie circostanze. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, vanno installati più cartelli.

In luoghi diversi dalle aree esterne il modello va integrato con almeno un avviso circostanziato che riporti gli elementi del predetto art. 13 con particolare riguardo alle finalità e all'eventuale conservazione.

Il supporto con l'informativa:

- deve essere collocato nei luoghi ripresi o nelle immediate vicinanze, non necessariamente a contatto con la telecamera;
- deve avere un formato e un posizionamento tale da essere chiaramente visibile;
- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati se le immagini sono solo visionate o anche registrate.

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, anche con un provvedimento generale, 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.

A questo fine, con il presente provvedimento il Garante prescrive a tutti i titolari del trattamento, quale misura opportuna per favorire il rispetto delle previsioni di legge (art. 143, comma 1, lett. c), del Codice), di sottoporre alla verifica preliminare di questa Autorità (anche in tal caso, con eventuali provvedimenti di carattere generale) i sistemi di videosorveglianza che prevedono una raccolta delle immagini collegata e/o incrociata e/o confrontata con altri particolari dati personali (ad esempio biometrici), oppure con codici identificativi di carte elettroniche o con dispositivi che rendono identificabile la voce.

La verifica preliminare del Garante occorre anche in caso di digitalizzazione o indicizzazione delle immagini (che rendono possibile una ricerca automatizzata o nominativa) e in caso di videosorveglianza c.d. dinamico-preventiva che non si limiti a riprendere staticamente un luogo, ma rilevi percorsi o caratteristiche fisionomiche (ad esempio riconoscimento facciale) o eventi improvvisi, oppure comportamenti anche non previamente classificati.

3.2.2. Autorizzazioni

I predetti trattamenti devono essere autorizzati preventivamente dal

Garante, anche attraverso autorizzazioni generali, quando riguardano dati sensibili o giudiziari, ad esempio in caso di riprese di persone malate o di detenuti (artt. 26 e 27 del Codice).

3.2.3. Altri esami preventivi

Non devono essere sottoposti all'esame preventivo del Garante, a meno che l'Autorità lo abbia disposto, i trattamenti di dati a mezzo videosorveglianza, fuori dei casi indicati nei precedenti punti 3.2.1. e 3.2.2. Non può desumersi alcuna approvazione implicita 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.

3.2.4. Notificazione

Gli stessi trattamenti devono essere notificati al Garante solo se rientrano in casi specificamente previsti (art. 37 del Codice). A tale riguardo l'Autorità ha disposto che non vanno comunque notificati i trattamenti relativi a comportamenti illeciti o fraudolenti, quando riguardano immagini o suoni conservati temporaneamente per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio (provv. n. 1/2004 del 31 marzo 2004, in G.U. 6 aprile 2004, n. 81 e in www.garanteprivacy.it; v. anche, sullo stesso sito, i chiarimenti forniti con nota n. 9654/33365 del 23 aprile 2004 relativamente alla posizione geografica delle persone).

3.3. Soggetti preposti e misure di sicurezza

3.3.1. Responsabili e incaricati

Si devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate ad utilizzare gli impianti e, nei casi in cui è indispensabile per gli scopi perseguiti, a visionare le registrazioni (art. 30 del Codice). Deve trattarsi di un numero molto ristretto di soggetti, in particolare quando ci si avvale di una collaborazione esterna.

Vanno osservate le regole ordinarie anche per ciò che attiene all'eventuale designazione di responsabili del trattamento, avendo particolare cura al caso in cui il titolare si avvalga di un organismo esterno anche di vigilanza privata (art. 29 del Codice).

La designazione di eventuali responsabili e incaricati "esterni" può essere effettuata solo se l'organismo esterno svolge prestazioni strumentali e subordinate alle scelte del titolare del trattamento. Questo non deve, ovviamente, essere un espediente per eludere la normativa in materia di protezione dei dati personali, come può accadere, per esempio, nel caso in cui la designazione dell'incaricato "esterno" mascheri una comunicazione di dati a terzi senza consenso degli interessati, oppure nel caso di diversità o incompatibilità tra le finalità perseguite dai soggetti che si scambiano i dati.

Quando i dati vengono conservati – naturalmente per un tempo limitato in applicazione del principio di proporzionalità – devono essere previsti diversi livelli di accesso al sistema e di utilizzo delle informazioni, avendo riguardo anche ad eventuali interventi per esigenze di manutenzione. Occorre prevenire possibili abusi attraverso opportune misure basate in particolare su una "doppia chiave" fisica o logica che consentano una immediata e integrale visione delle immagini solo in caso di necessità (da parte di addetti alla manutenzione o per l'estrazione dei dati ai fini della difesa di un diritto o del riscontro ad una istanza di accesso, oppure per assistere la competente Autorità giudiziaria o di polizia giudiziaria). Va infatti tenuto conto che l'accessibilità regolamentata alle immagini registrate da parte degli addetti è fattore di sicurezza.

Sono infine opportune iniziative periodiche di formazione degli incaricati sui doveri, sulle garanzie e sulle responsabilità, sia all'atto dell'introduzione del sistema di videosorveglianza, sia in sede di modifiche delle modalità di utilizzo (cfr. Allegato B) al Codice, regola n. 19.6).

3.3.2. Misure di sicurezza

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 o trattamento non consentito o non conforme alle finalità della raccolta (art. 31 del Codice).

Alcune misure, c.d. "misure minime", sono obbligatorie anche sul piano penale. Il titolare del trattamento che si avvale di un soggetto esterno deve ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle regole in materia (artt. 33-36 e 169, nonché Allegato B) del Codice, in particolare punto 25; v. anche i chiarimenti forniti con nota n. 6588/31884 del 22 marzo 2004, in www.garanteprivacy.it).

3.4. Durata dell'eventuale conservazione

In applicazione del principio di proporzionalità (v. anche art. 11, comma 1, lett. e), del Codice), anche l'eventuale conservazione temporanea dei dati deve essere commisurata al grado di indispensabilità e per il solo 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 specifici 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), è ammesso un tempo più ampio di conservazione dei dati, che non può comunque superare la settimana.

Un 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 dall'Autorità giudiziaria o di polizia giudiziaria in relazione ad un'attività investigativa in corso.

Il sistema impiegato deve essere programmato in modo da operare al momento prefissato – ove tecnicamente possibile – la cancellazione automatica da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

3.5. Documentazione delle scelte

Le ragioni delle scelte, cui si è fatto richiamo, 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.

3.6. 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 e di ottenere l'interruzione di un trattamento illecito, in specie quando non sono adottate idonee misure di sicurezza o il sistema è utilizzato da persone non debitamente autorizzate (art. 7 del Codice).

La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti alla persona istante identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal Codice (art. 10, commi 3 s., del Codice). A tal fine può essere opportuno che la verifica dell'identità del richiedente avvenga mediante esibizione o allegazione di un documento di riconoscimento che evidenzi un'immagine riconoscibile dell'interessato.

4. Settori specifici

4.1. Rapporti di lavoro

Nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa e ciò anche in caso di erogazione di servizi per via telematica mediante c.d. "web contact center". Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è impiegata per esigenze organizzative e dei processi

produttivi, ovvero è richiesta per la sicurezza del lavoro (art. 4 legge n. 300/1970; art. 2 d.lgs. n. 165/2001).

Queste garanzie vanno osservate sia all'interno degli edifici, sia in altri luoghi di prestazione di lavoro, così come, ad esempio, si è rilevato in precedenti provvedimenti dell'Autorità a proposito di telecamere installate su autobus (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).

È inammissibile l'installazione di sistemi di videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all'attività lavorativa (ad esempio bagni, spogliatoi, docce, armadietti e luoghi ricreativi).

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 e altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull'attività giornalistica contenute nel Codice, fermi restando, comunque, i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l'osservanza del codice deontologico per l'attività giornalistica e il diritto del lavoratore a tutelare la propria immagine opponendosi anche, per motivi legittimi, alla sua diffusione.

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 esempio unità di rianimazione), stante la natura sensibile di molti dati che possono essere in tal modo raccolti, devono essere limitati ai casi di stretta indispensabilità e circoscrivendo le riprese solo a determinati locali e a precise fasce orarie; 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 delle doverose misure che il Codice prescrive per le strutture sanitarie (art. 83).

Il titolare deve garantire che possano accedere alle immagini solo i soggetti specificamente autorizzati (ad esempio personale medico e infermieristico) e che le stesse non possano essere visionate da estranei (ad esempio visitatori). Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di familiari di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (ad esempio rianimazione), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto.

Le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse, a pena di sanzione penale (artt. 22, comma 8, e 167 del Codice). Va assolutamente evitato il rischio di diffusione delle

immagini di persone malate su monitor collocati in locali liberamente accessibili al pubblico.

Nei casi in cui l'impiego di un sistema di videosorveglianza all'interno di una struttura sanitaria non sia finalizzato alla cura del paziente, bensì solo a finalità amministrative o di sicurezza (ad esempio il controllo dell'edificio o di alcuni locali), e sia possibile che attraverso lo stesso siano raccolte immagini idonee a rivelare lo stato di salute, il soggetto pubblico titolare deve menzionare tale trattamento nell'atto regolamentare sui dati sensibili da adottare in base al Codice (art. 20).

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) e tenere conto della delicatezza dell'eventuale trattamento di dati relativi a minori.

A tal fine, se può risultare ammissibile il loro utilizzo in casi di stretta indispensabilità (ad esempio a causa del protrarsi di atti vandalici), gli stessi devono essere circoscritti alle sole aree interessate e attivati negli orari di chiusura degli istituti, regolando rigorosamente l'eventuale accesso ai dati.

Restano di competenza dell'Autorità giudiziaria o di polizia le iniziative intraprese a fini di tutela dell'ordine pubblico o di individuazione di autori di atti criminali (ad esempio spacciatori di stupefacenti, adescatori, ecc.).

4.4. Luoghi di culto e di sepoltura

L'installazione di sistemi di videosorveglianza presso chiese o altri luoghi di culto o di ritrovo di fedeli deve essere oggetto di elevate cautele, 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, 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.

5. Soggetti pubblici

5.1. Svolgimento di funzioni istituzionali

Un soggetto pubblico può effettuare attività di videosorveglianza solo e esclusivamente per svolgere funzioni istituzionali che deve individuare e esplicitare con esattezza e di cui sia realmente titolare in base all'ordinamento di riferimento (art. 18, comma 2, del Codice).

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 (art. 19, comma 2, del Codice).

Tale circostanza si è ad esempio verificata presso alcuni enti locali che dichiarano di perseguire direttamente, in via amministrativa, finalità di prevenzione e accertamento dei reati che competono alle Autorità giudiziarie e alle Forze di polizia. Vanno richiamate quindi in questa sede le riflessioni già suggerite in passato a proposito di talune ordinanze comunali in tema di prostituzione in luoghi pubblici (v. provv. 26 ottobre 1998, in Bollettino del Garante n. 6/1998, p. 131).

Benché effettuata per la cura di un interesse pubblico, la videosorveglianza deve rispettare i principi già richiamati.

Quando il soggetto è realmente titolare di un compito, attribuito dalla legge in materia di sicurezza pubblica o di accertamento, prevenzione e repressione di reati, per procedere ad una videosorveglianza di soggetti identificabili deve ricorrere un'esigenza effettiva e proporzionata di prevenzione o repressione di pericoli concreti e specifici di lesione di un bene (ad esempio in luoghi esposti a reale rischio o in caso di manifestazioni che siano ragionevolmente fonte di eventi pregiudizievoli).

Non risulta quindi lecito procedere, senza le corrette valutazioni richiamate in premessa, ad una videosorveglianza capillare di intere aree cittadine "cablate", riprese integralmente e costantemente e senza adeguate esigenze. Del pari è vietato il collegamento telematico tra più soggetti, a volte raccordati ad un "centro" elettronico, che possa registrare un numero elevato di dati personali e ricostruire interi percorsi effettuati in un determinato arco di tempo.

Risulta parimenti priva di giustificazione l'installazione di impianti di videosorveglianza al solo fine (come risulta da casi sottoposti al Garante), di controllare il rispetto del divieto di fumare o gettare mozziconi, di calpestare aiuole, di affiggere o di fotografare, o di altri divieti relativi alle modalità nel depositare i sacchetti di immondizia entro gli appositi contenitori.

Le specifiche norme di legge o di regolamento e le funzioni legittimamente individuate dall'ente costituiscono l'ambito operativo entro il quale il trattamento dei dati si intende consentito. Come prescritto dal Codice, l'eventuale comunicazione a terzi è lecita solo se espressamente prevista da una norma di legge o di regolamento (art. 19, comma 3, del Codice).

Il Codice individua poi specifiche regole volte invece a consentire, in un quadro di garanzie, riprese audio-video a fini di documentazione dell'attività istituzionale di organi pubblici (artt. 20-22 e 65 del Codice).

Salvo i casi previsti per le professioni sanitarie e gli organismi sanitari, il soggetto pubblico non deve richiedere la manifestazione del consenso degli interessati (art. 18, comma 4, del Codice).

5.2. Informativa

Contrariamente a quanto prospettato da alcuni enti locali, l'informativa agli interessati deve essere fornita nei termini illustrati nel paragrafo 3.1. e non solo mediante pubblicazione sull'albo dell'ente, oppure 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.

5.3 Accessi a centri storici

Qualora introducano sistemi di rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato, i Comuni dovranno rispettare quanto dettato dal d.p.r. 22 giugno 1999, n. 250. Tale normativa impone ai Comuni di richiedere una specifica autorizzazione amministrativa, nonché di limitare la raccolta dei dati sugli accessi rilevando le immagini solo in caso di infrazione (art. 3 d.p.r. n. 250/1999).

I dati trattati possono essere conservati solo per il periodo necessario per contestare le infrazioni e definire il relativo contenzioso e si può accedere ad essi solo a fini di polizia giudiziaria o di indagine penale.

5.4. Sicurezza nel trasporto urbano

Alcune situazioni di particolare rischio fanno ritenere lecita l'installazione su mezzi di trasporto pubblici di sistemi di videosorveglianza. Tali sistemi di rilevazione sono leciti anche presso talune fermate di mezzi urbani specie in aree periferiche che spesso sono interessate da episodi di criminalità (aggressioni, borseggi, ecc.).

Valgono, anche in questi casi, le considerazioni già espresse a proposito della titolarità in capo alle sole Forze di polizia dei compiti di accertamento, prevenzione e accertamento di reati, nonché del diritto di accesso alle immagini conservate per alcune ore, cui si dovrebbe accedere solo in caso di illeciti compiuti.

Negli stessi casi, deve osservarsi particolare cura anche per ciò che riguarda l'angolo visuale delle apparecchiature di ripresa, nella collocazione di idonee informative a bordo dei veicoli pubblici e nelle aree di fermata – presso cui possono transitare anche soggetti estranei – e per quanto attiene alla ripresa sistematica di dettagli o di particolari non rilevanti riguardanti i passeggeri.

5.5. Deposito dei rifiuti

In applicazione dei principi richiamati, il controllo video di aree abusivamente impiegate come discariche di materiali e di sostanze pericolose è lecito se risultano inefficaci o inattuabili altre misure. Come già osservato, il medesimo controllo non è invece lecito – e va effettuato in altra forma – se è volto ad accertare solo infrazioni amministrative rispetto a disposizioni concernenti modalità e orario di deposito dei rifiuti urbani.

6. Privati e enti pubblici economici

6.1. Consenso

A differenza dei soggetti pubblici, i privati e gli enti pubblici economici possono trattare dati personali solo se vi è il consenso preventivo espresso dall'interessato, oppure uno dei presupposti di liceità previsti in alternativa al consenso (artt. 23 e 24 del Codice).

In caso di impiego di strumenti di videosorveglianza da parte di privati e 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 esempio di sicurezza o di deterrenza) che non si conciliano con richieste di esplicita accettazione da parte di chi intende accedere a determinati luoghi o usufruire di taluni servizi.

Il consenso, oltre alla presenza di un'informativa preventiva e idonea, è valido solo se espresso e documentato per iscritto. Non è pertanto valido un consenso presunto o tacito, oppure manifestato solo per atti o comportamenti concludenti, consistenti ad esempio nell'implicita accettazione delle riprese in conseguenza dell'avvenuto accesso a determinati luoghi.

Nel settore privato, fuori dei casi in cui sia possibile ottenere un esplicito consenso libero, espresso e documentato, vi può essere la necessità di verificare se esista un altro presupposto di liceità utilizzabile in alternativa al consenso, come indicato nel paragrafo successivo.

6.2. Bilanciamento degli interessi

6.2.1. Profili generali

Un'idonea alternativa all'esplicito consenso va 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 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.

Considerata l'ampia serie di garanzie e condizioni sopra indicate, non appare necessario che il Garante, per alcuni trattamenti in ambito privato di seguito indicati, prescriva ulteriori condizioni e limiti oltre quelli già richiamati in premessa.

6.2.2. Registrazione delle immagini

I trattamenti di dati possono essere più invasivi rispetto alla semplice rilevazione, qualora siano registrati su supporti oppure abbinati ad altre fonti o conservati in banche di dati, talora solo per effetto di un dispositivo di allarme programmato. E ciò in considerazione delle molteplici attività di elaborazione cui i dati possono essere sottoposti anche ad altri fini.

In presenza di concrete e effettive situazioni di rischio tali registrazioni sono consentite a protezione delle persone, della proprietà o del patrimonio aziendale (ad esempio rispetto a beni già oggetto di ripetuti e gravi illeciti), relativamente all'erogazione di particolari servizi pubblici (si pensi alle varie forme di trasporto) o a specifiche attività (che si svolgono ad esempio in luoghi pubblici o aperti al pubblico, o che comportano la presenza di denaro o beni di valore, o la salvaguardia del segreto aziendale od industriale in relazione a particolari tipi di attività).

6.2.3. Videosorveglianza senza registrazione

Nei casi in cui le immagini sono unicamente visionate in tempo reale, oppure conservate solo per poche ore mediante impianti a circuito chiuso (CCTV), possono essere tutelati legittimi interessi rispetto a concrete e effettive situazioni di pericolo per la sicurezza di persone e beni, anche quando si tratta di esercizi commerciali esposti ai rischi di attività criminali in ragione della detenzione di denaro, valori o altri beni (ad esempio gioiellerie, supermercati, filiali di banche, uffici postali). La videosorveglianza può risultare eccedente e sproporzionata quando sono già adottati altri efficaci dispositivi di controllo o di vigilanza oppure quando vi è la presenza di personale addetto alla protezione.

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

6.2.4. Videocitofoni

Sono ammissibili per identificare coloro che si accingono ad entrare in luoghi privati videocitofoni o altre apparecchiature che rilevano immagini o suoni senza registrazione. Tali apparecchiature 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 (art. 5, comma 3, del Codice).

Altri dispositivi di rilevazione e controllo, invece, spesso non sono facilmente individuabili anche per mancanza di informativa, né la loro collocazione è altrimenti segnalata. In alcuni casi, poi, più telecamere

collocate anche all'interno di un edificio (pianerottoli, corridoi, scale) si attivano contemporaneamente e, sia pure per un tempo limitato, riprendono le persone fino all'ingresso negli appartamenti. Anche in questi casi è necessaria una adeguata informativa.

6.2.5. Riprese nelle aree comuni

L'installazione degli strumenti descritti nel paragrafo precedente, se effettuata nei pressi di immobili privati e all'interno di condominii e loro pertinenze (es. posti auto, box), benché non sia soggetta al Codice quando i dati non sono comunicati sistematicamente o diffusi, richiede comunque l'adozione di cautele a tutela dei terzi (art. 5, comma 3, 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 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 relative ad aree comuni (cortili, pianerottoli, scale, garage comuni) o antistanti l'abitazione di altri condomini.

Il Codice trova invece applicazione in caso di utilizzazione di un sistema di ripresa di aree condominiali da parte di più proprietari o condomini, oppure da un condominio, dalla relativa amministrazione (comprese le amministrazioni di residence o multiproprietà), da studi professionali, società o da enti no-profit.

L'installazione di questi impianti è ammissibile esclusivamente in relazione all'esigenza di preservare la sicurezza di persone e la tutela di beni da concrete situazioni di pericolo, di regola costituite da illeciti già verificatisi, oppure nel caso di attività che comportano, ad esempio, la custodia di denaro, valori o altri beni (recupero crediti, commercio di preziosi o di monete aventi valore numismatico).

La valutazione di proporzionalità va effettuata anche nei casi di utilizzazione di sistemi di videosorveglianza che non prevedano la registrazione dei dati, in rapporto ad altre misure già adottate o da adottare (ad esempio sistemi comuni di allarme, blindatura o protezione rinforzata di porte e portoni, cancelli automatici, abilitazione degli accessi).

7. Prescrizioni e sanzioni

Il Garante invita tutti gli operatori interessati ad attenersi alle prescrizioni illustrate e a quelle definite opportune parimenti indicate nel presente provvedimento, in attesa dei più specifici interventi che potranno derivare in materia da un c.d. provvedimento di verifica preliminare di questa Autorità (art. 17 del Codice), oppure dal codice deontologico che il Garante ha promosso per disciplinare in dettaglio altri aspetti del trattamento dei dati personali effettuato "con strumenti elettronici di rilevamento di immagini" (art. 134 del Codice).

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, e 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 s. del Codice).

TUTTO CIÒ PREMESSO IL GARANTE:

1. prescrive ai titolari del trattamento nei settori interessati, ai sensi dell'art. 154, comma 1, lett. c), del Codice, le misure necessarie e opportune indicate nel presente provvedimento al fine di rendere il trattamento conforme alle disposizioni vigenti;
2. individua, nei termini di cui in motivazione, ai sensi dell'art. 24, comma 1, lett. f) del Codice, i casi nei quali il trattamento dei dati personali mediante videosorveglianza può essere effettuato da soggetti privati e enti pubblici economici, nei limiti e alle condizioni indicate, per perseguire legittimi interessi e senza richiedere il consenso degli interessati;
3. individua in allegato un modello semplificato di informativa utilizzabile alle condizioni indicate in motivazione.

Roma, 29 aprile 2004

2. Circolare ministeriale
n. 558/A/421.2/70/456

Oggetto: Sistemi di videosorveglianza. Definizione di linee guida in materia

Il recente sviluppo del settore della videosorveglianza risponde ad avvertite necessità di sicurezza e è stato determinato, in molti casi, dalle esigenze di implementazione tecnologica del sistema di controllo del territorio e di diffusione della legalità, sia per effetto dell'impatto nelle Regioni del Sud delle misure del Programma Operativo Sicurezza per lo sviluppo del Mezzogiorno, sia in virtù di accordi siglati in materia con le Amministrazioni locali e regionali allo scopo di contrastare fenomeni di criminalità, inciviltà e disordine urbano, sia infine per effetto di iniziative nel mondo produttivo e delle associazioni.

Il moltiplicarsi delle iniziative in questione da parte di privati, associazioni di categoria e enti locali, può ben considerarsi segno tangibile del generale consenso incontrato dalla politica di valorizzazione e integrazione di tutte le risorse disponibili, pubbliche e private, perseguita dall'Amministrazione dell'interno allo scopo di rafforzare il sistema nazionale della pubblica sicurezza, coinvolgendo, in una logica partecipativa avanzata, tutti i soggetti pubblici e privati interessati.

Ciò nondimeno, la complessità del quadro emergente dalle diverse iniziative induce a considerare quanto mai necessaria e urgente un'azione volta ad armonizzare e razionalizzare le iniziative in parola, tenendo conto delle diverse esigenze di carattere primario in gioco:

- la doverosa considerazione e tutela dei diritti dei cittadini e, quindi, la tutela della riservatezza dei dati personali, secondo le linee d'azione predisposte dal Garante per la protezione dei dati in questione, con il "decalogo" del 29 novembre 2000 e, da ultimo, con il provvedimento generale del 29 aprile 2004, al quale si fa rinvio;
- il rispetto delle competenze dei soggetti pubblici interessati, a garanzia anche dell'efficacia degli interventi, secondo linee di imputazione coerenti con le rispettive attribuzioni e tipologie d'intervento;
- la garanzia tecnico-operativa dell'efficacia dei sistemi, soprattutto quando essi siano in qualsiasi modo collegati con le Sale o Centrali operative delle Forze di polizia;
- l'armonizzazione, infine, delle esigenze della sicurezza primaria, di cui primi garanti sono le Forze di polizia dello Stato, con l'evoluzione del "sistema" verso il ricorso sempre più frequente a forme di sicurezza partecipata e sussidiaria.

La presente direttiva attiene in particolar modo a questi ultimi aspetti, avendo di mira i sistemi di videosorveglianza adottati dalle Forze di polizia per il controllo del territorio e quelli che, pur adottati da soggetti pubblici o privati diversi, per l'essere comunque funzionali all'attività delle Autorità di pubblica sicurezza e degli Organi di polizia, sono stati sinora attestati, in base a strumenti pattizi, in tutto o in parte, anche in

funzione di teleallarme, presso le Sale o Centrali operative degli Organi di polizia a competenza generale.

Essa non incide, pertanto, sulle autonome valutazioni dei privati e dei soggetti pubblici, anche locali, relativamente alle videosorveglianze e ai sistemi di teleallarme di specifico e esclusivo interesse, attivate e gestite integralmente con mezzi propri, nell'ambito delle vigenti disposizioni in materia di vigilanza privata e, rispettivamente, dei compiti di pertinenza degli enti locali e degli altri soggetti pubblici interessati.

Nella sopra delineata prospettiva, di più diretto interesse istituzionale, un primo profilo sul quale occorre attirare l'attenzione delle SS.LL. riguarda, innanzi tutto, la fase relativa alla scelta di attivare o meno un sistema di videosorveglianza.

A questo proposito, si conferma l'esigenza di una stretta interrelazione fra l'impiego di tali apparati e le effettive necessità di prevenzione e repressione dei reati e degli altri illeciti rilevanti per l'ordine e la sicurezza pubblica, e quelle di pronto intervento ai fini della sicurezza e del soccorso pubblico, senza di cui verrebbero meno i criteri della necessità, della pertinenza e della non eccedenza dei dati e dei relativi trattamenti, statuiti dal codice in materia di protezione dei dati personali.

Conseguentemente, anche la scelta delle aree dovrà essere particolarmente oculata, nell'ambito di un procedimento che veda interessati i Comitati Provinciali per l'ordine e la sicurezza pubblica, eventualmente allargati ai responsabili delle Amministrazioni dello Stato e degli enti locali interessati, ai sensi dell'art.16 della l. n.128/2001.

In seno ai Comitati potranno essere esaminate le effettive esigenze e la concreta utilità degli apparati di telecontrollo, anche al fine di evitarne un'ingiustificata proliferazione, valorizzando gli esiti valutativi emergenti dall'attuazione dei piani coordinati di controllo del territorio, particolarmente in relazione ad aree nelle quali sia stata evidenziata la necessità di potenziare l'attività di prevenzione.

Criteri altrettanto scrupolosi saranno adottati per quanto concerne l'attivazione di sistemi di telecontrollo che coinvolgono le Sale o Centrali operative delle Forze di polizia a competenza generale, al fine di garantire, insieme alla compatibilità tecnica dei sistemi di visione, allarme e trasmissione dei dati con le tecnologie in uso presso le predette Sale o Centrali, l'efficienza e funzionalità del sistema, anche in sede di intervento operativo.

Sotto il profilo tecnologico, in particolare, si rinvia alla nota tecnica allegata recante i relativi parametri di compatibilità. Sotto quello funzionale, si richiama l'attenzione sul fatto che lo sviluppo degli apparati di videosorveglianza deve coniugarsi con l'esigenza di garantire l'efficacia e la tempestività della risposta delle Forze di polizia, a fronte delle situazioni emergenti. Per questo motivo i collegamenti con le Sale o Centrali operative dovranno essere necessariamente circoscritti, indipendentemente dalle tecnologie applicate, in considerazione dell'articolazione organizzativa e funzionale delle stesse Forze di polizia, necessariamente dimensionata sulle risorse disponibili e sulle complessive esigenze di sicurezza del territorio.

La diretta visualizzazione delle immagini rilevate dai sistemi in parola nelle Sale o Centrali operative potrà essere, quindi, mantenuta nei soli casi, rigorosamente limitati, di obiettivi "istituzionali" particolarmente sensibili, che fanno parte di una configurazione sistemica dei mezzi di allarme e di intervento a tutela dell'ordine e della sicurezza pubblica, o di obiettivi di interesse strategico per la sicurezza primaria.

Qualora le esigenze di videosorveglianza e teleallarme non implichino l'osservanza dei rigorosi criteri sopra enunciati, e sempre che sussistano i requisiti di pubblico interesse (necessità, pertinenza, non eccedenza dei dati e dei trattamenti) sopra delineati, potrà essere valutata una soluzione mediata, in forza della quale il flusso delle immagini prodotte dai sistemi giunga, a seconda degli obiettivi da vigilare e nel fondamentale rispetto delle competenze istituzionali, presso gli Organi di polizia locale ovvero presso Istituti di vigilanza, in grado di garantire i servizi di monitoraggio e il conseguente, eventuale allertamento della Sala o Centrale operativa delle Forze di polizia, nei casi in cui vengano riscontrati allarmi o anomalie.

Nel contesto delineato, il ruolo delle Forze di polizia sarà quindi ricondotto alla fisiologia dell'attivazione delle adeguate misure di intervento in seguito all'allertamento cui il soggetto deputato al monitoraggio dei sistemi provvederà quando le immagini ne indichino l'effettiva esigenza, ovvero, fuori della flagranza del reato o di un fatto comunque lesivo dell'ordine e della sicurezza pubblica, alla acquisizione, per l'esame investigativo, delle immagini o altri segnali relativi a possibili situazioni di rischio, eventualmente detenuti in conformità alle sopra ricordate linee d'azione predisposte dal Garante.

Nello specifico, il soggetto che propone l'attivazione dei sistemi di videosorveglianza, oltre ad approvvigionarsi di adeguata strumentazione, connettività e relativa manutenzione, dovrà provvedere, nella rigorosa osservanza della normativa posta a tutela dei dati personali, anche ai servizi di gestione, memorizzazione e monitoraggio delle immagini, provvedendo all'allertamento immediato dell'Organo di polizia nei casi di effettiva esigenza e mettendo, comunque, a sua disposizione, come detto, i segnali e le immagini relative a situazioni di rischio, appositamente selezionate, ivi comprese le registrazioni dei fatti che, anche fuori della flagranza del reato, presentino anomalie suscettibili di interesse investigativo, come potrebbe verificarsi nel caso delle registrazioni di attività che, ad un successivo approfondimento, possono risultare fasi preparatorie di un'azione criminosa e concorrere alla individuazione dei colpevoli.
Resta inteso che anche la conservazione di quest'ultima documentazione dovrà conformarsi a criteri temporali ben precisi, correlati alla durata delle indagini.

Premesso che per gli impianti di videosorveglianza che non siano di pertinenza diretta dell'Amministrazione ogni onere finanziario, compreso quello connesso alla gestione del sistema, deve essere interamente soddisfatto dall'ente o altro soggetto proponente, si sottolinea che, nel caso di connessione diretta, il soggetto medesimo dovrà farsi carico altresì degli oneri di approvvigionamento, connessione e manutenzione relativi agli apparati dedicati alla specifica esigenza posti a disposizione delle Forze di polizia.

In relazione a quanto sopra, le SS.LL. vorranno curare che le Forze di polizia, comprese quelle a competenza specialistica, e tutti i soggetti (enti territoriali, associazioni di categoria e privati) che interagiscono con le stesse nella realizzazione dei progetti di videosorveglianza, osservino strettamente i criteri sopra delineati, che rispondono ai principi di carattere generale perseguiti dall'Amministrazione, sui quali si ritiene utile soffermare, qui di seguito, l'attenzione con alcune conclusive considerazioni.

Premesso che un incremento generale della sicurezza delle città e dei cittadini deve puntare necessariamente sullo sviluppo di politiche integrate della prevenzione, anche attraverso una maggiore sinergia fra la "sicurezza primaria" propria degli organi specificamente preposti alla sicurezza pubblica, gli Organi di polizia locale, nell'ambito dei rispettivi compiti istituzionali, e gli operatori della "sicurezza sussidiaria", con particolare riguardo agli Istituti di vigilanza privata, va sottolineata la necessità di un'attenta considerazione dei diversi ambiti istituzionali, intesa a prevenire che i sistemi di controllo partecipato possano alterare il corretto rapporto tra gli stessi.

In tale quadro, nel ribadire che – salvo che per gli obiettivi istituzionali o di interesse strategico per la sicurezza primaria – l'attività di gestione e di controllo degli apparati di videosorveglianza deve essere effettuata dalle Polizie locali o dagli Istituti di vigilanza privata, a seconda degli obiettivi da vigilare, vanno evidenziati la funzione integratrice e il ruolo di complessivo potenziamento funzionale di tale soluzione alternativa e "mediata", che potrà – ove ritenuto dalle SS.LL. in relazione alle circostanze e alle disponibilità locali, e anche sulla base di specifiche intese – essere implementata con collegamenti diretti per particolari esigenze di carattere assolutamente contingente. Le SS.LL. vorranno valutare, in ogni caso, l'opportunità di promuovere una specifica attività formativa per il personale addetto agli apparati di videosorveglianza, contemplando altresì, in funzione delle finalità di prevenzione generale perseguite, per quello non appartenente alle Forze di polizia, la possibilità di collaborazione da parte delle stesse nel suddetto percorso formativo.

Gli enunciati principi generali, che attengono anche alle convenzioni sviluppate nell'ambito dei progetti di telecontrollo connessi al Programma Operativo Sicurezza per lo sviluppo del Mezzogiorno, devono intendersi riferiti a tutti i protocolli sottoscritti e sono, in ogni caso, vincolati all'osservanza delle note direttive ministeriali in tema di raccordo con gli organi centrali.

PEL MINISTRO

IL CAPO DELLA POLIZIA DIRETTORE GENERALE
DELLA PUBBLICA SICUREZZA (De Gennaro)

SISTEMI DI VIDEOSORVEGLIANZA – Nota Tecnica

Premessa fondamentale è che l'installazione di sistemi di videosorveglianza facenti capo a strutture pubbliche e private deve essere realizzata nella piena compatibilità con le tecnologie adottate nelle Sale/Centrali operative delle Forze di polizia.

Tali impianti sono destinati ad assolvere funzioni riconducibili essenzialmente a:

a. Osservazione diretta da remoto. Gli apparati consentono di osservare una determinata area quando, in presenza di particolari eventi, se ne ravvisi l'esigenza (ad esempio transito di pubbliche manifestazioni nella zona servita dall'impianto). Al riguardo, è assolutamente necessario che il tempo di trasmissione dell'immagine, tra l'accadimento reale e quello visualizzato dall'operatore, sia ridotto al minimo.
b. Videosorveglianza. Il sistema effettua una vera e propria attività di vigilanza su persone e beni, sostituendo, in tutto o in parte, la presenza umana sul posto. La relativa strumentazione deve prevedere l'impiego di:
   – sensori meccanici o elettromagnetici esterni alle telecamere (ad esempio per la possibilità di rilevare il transito o la sosta di una autovettura);
   – sistemi per la registrazione delle sorgenti video in continuo o su allarme;
   – sistemi software di variazione e analisi delle immagini (ad esempio per la capacità di rilevare l'asportazione di un oggetto o, tra tante persone in piedi, la presenza di una sdraiata).

Le tecnologie hardware e software devono permettere la gestione automatica di "allarmi video".

Di seguito, sono riportate specifiche indicazioni tecniche per l'installazione e l'integrazione degli impianti di videosorveglianza con i sistemi in uso nelle Sale/Centrali operative:
– l'invio dei segnali video dalle strutture pubbliche e private verso le Sale/Centrali operative delle Forze di polizia deve essere convogliato con un unico collegamento fisico, il cui protocollo di comunicazione sia di tipo IP, dimensionato con una larghezza di banda adeguata al numero di sorgenti video gestite e comunque in grado di visualizzare, in modalità "full motion" (diretta), almeno una singola sorgente video;
– presso le menzionate Sale/Centrali operative deve essere presente un software per la gestione delle sorgenti video, che risponda alle seguenti caratteristiche:

- visualizzazione (anche di immagini multiple) di tutte le telecamere che afferiscono al server di videosorveglianza;

- visualizzazione automatica, con segnalazione di allarme audio e visivo, di immagini video provenienti da una telecamera per la quale si siano verificate condizioni di allarme;

- registrazione (e riproduzione) delle immagini di una o più sorgenti video, in modalità manuale (gestita dall'operatore) e automatica (al verificarsi dell'allarme e/o su rilevazione di movimento);
- comunicazione con il sistema Video Server presente presso le strutture pubbliche e private con protocollo IP;
- fruibilità delle interfacce software (API – Application Programming Interface), per l'integrazione con sistemi già presenti presso le Sale/Centrali operative;
- compatibilità del software con i sistemi operativi (Windows 2000 e XP) utilizzati presso le Sale/Centrali operative;
- le comunicazioni IP tra la componente software delle Sale/Centrali operative e i Video Server presenti presso le strutture pubbliche e private devono avere un alto livello di sicurezza e riservatezza (ad esempio connessioni SSL Secure Socket Layer).

Finito di stampare
nel mese di maggio 2006