****

IL DIRETTORE AMMINISTRATIVO
Massimo Mancini

Visto, esprime parere _____

IL DIRETTORE SANITARIO
Vito Gregorio Colacicco

Visto, esprime parere _____

IL COMMISSARIO STRAORDINARIO
Angelo Domenico Colasanto

La presente deliberazione è trasmessa al Collegio Sindacale e viene pubblicata sul sito web aziendale nel rispetto di quanto disposto dalla L.R. n. 40/2007

IL RESPONSABILE DELLA SEGRETERIA

Si dichiara che il presente atto è copia conforme all'originale
Esso è composto da n. 51 fogli

Bari, - 3 AGO. 2011

Il Funzionario Coordinatore
della Segreteria Direzionale
A.S.L. BA
(Sig. Giuseppe Colella)

REGIONE PUGLIA
ASL BA

AZIENDA SANITARIA LOCALE DELLA PROVINCIA DI BARI

DELIBERAZIONE DEL COMMISSARIO STRAORDINARIO

Deliberazione n. 1461 del - 3 AGO. 2011

OGGETTO: **Adempimenti <Codice della Privacy> ex d.lgs 196/2003 e s.m.i. *"Regolamento e Modulistica per Videosorveglianza aziendale"***

L'anno 2011, il giorno tre del mese di agosto in Bari, nella sede della A.S.L. al Lungomare Starita n. 6,

IL COMMISSARIO STRAORDINARIO

- Visto il D.Lgs. 30/12/1992 n. 502 e successive integrazioni e modifiche;
- Vista la Legge Regionale 28/12/1994 n. 36;
- Vista la Legge Regionale 30/12/1994 n. 38
- Vista la Legge Regionale 03/08/2006 n. 25;
- Vista la Legge Regionale 28/12/2006 n. 39;
- Vista la Deliberazione della Giunta Regionale n. 1472 del 28.06.2011

Sulla base di conforme istruttoria dell'Ufficio Tutela della Privacy

HA ADOTTATO

Il seguente provvedimento

Premesso che:

- il d.lgs 30.6.2003, n. 196 "Codice in materia di protezione dei dati personali":

- garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali (art. 2);
- definisce "il Responsabile" come la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento dei dati personali (art. 4, co. 1, lett. g);
- pone a carico dell'Azienda l'obbligo di adottare le misure minime di sicurezza individuate dal "Codice in materia di protezione dei dati personali";

Considerato che:

- la direzione Strategica Aziendale ritiene opportuno dotare l'ASL di Bari di un "*Regolamento per sistema di videosorveglianza e relativa modulistica*", nel rispetto :

- della normativa del Codice della Privacy (d.lgs n. 196/2003 e s.m.i.);
- Provvedimento Garante della Privacy del 29 aprile 2004;
- Provvedimento Garante della Privacy dell'8 aprile 2010;
- Decalogo di regole dettate dal Garante della Privacy in materia di videosorveglianza del 29 novembre 2010;
- Del vademecum redatto dal Garante della Privacy (presente all'indirizzo www.garanteprivacy.it - sezione videosorveglianza -);

Preso atto che:

- in data 26 aprile c.a. la società "Studiodelta" di Bari ha depositato presso il protocollo generale dell'Azienda (prot. in arrivo n. 71440 del 26.04.2011 che si allega in copia al presente provvedimento) una bozza di <*Regolamento per Sistemi di Videosorveglianza*> e relativa modulistica, che include, tra l'altro, anche gli indirizzi forniti in materia dal Garante della Privacy;

Dato atto che:

- dal presente provvedimento non derivano oneri per l'Azienda;

Tanto premesso:

- si propone l'adozione del presente provvedimento che stabilisce per l'ASL di Bari il <*Regolamento per Sistemi di Videosorveglianza*>;
- si precisa fin d'ora che il <*Regolamento per Sistemi di Videosorveglianza*> potrà essere successivamente modificato e/o integrato a seguito di successivi chiarimenti del Garante della Privacy, suggerimenti offerti dai Responsabili del Trattamento della ASL di Bari ovvero sulla base di nuove e diverse esigenze organizzative aziendali;

Acquisiti i pareri del Direttore Amministrativo e del Direttore Sanitario

D E L I B E R A

-per le ragioni precisate in narrativa che qui si intendono integralmente riportate e confermate -

A) di prendere atto che il Garante della Privacy in materia di videosorveglianza ha emanato i seguenti documenti: Provvedimento Garante della Privacy del 29 aprile 2004; Provvedimento Garante della Privacy dell'8 aprile 2010; Decalogo di regole dettate dal Garante della Privacy in data 29 novembre 2010; vademecum redatto dal Garante della Privacy (documenti tutti allegati al presente provvedimento per farne parte integrante);

B) di recepire il <*Regolamento per Sistemi di Videosorveglianza*> e relativa modulistica predisposto dalla società "Studiodelta" di Bari che si intende qui per ritrascritto e parte integrante del presente provvedimento;

C) di trasmettere il presente atto al Dirigente URP per curare l'inserimento delle istruzioni sul sito aziendale www.asl.bari.it - sezione privacy -;

D) di dare mandato al Responsabile dell'Ufficio Tutela della Privacy, Avv. Luigi Fruscio, di trasmettere la presente deliberazione ai Responsabili del Trattamento della ASL di Bari corredata dei documenti allegati;

E) che i Responsabili del Trattamento devono rendere massima divulgazione al <*Regolamento per Sistemi di Videosorveglianza*> e relativa modulistica, nelle strutture di appartenenza per gli utenti/cittadini, gli incaricati del trattamento e i dipendenti;

F) dare atto che dal presente provvedimento non derivano oneri per l'Azienda;

Il Responsabile
Ufficio Tutela della Privacy
Avv. Luigi Fruscio

Servizio di Consulenza organizzativo-gestionale in materia di Privacy
STUDIODELTA Srl

ASL BA
U.O.R. 01 - Direzione Generale
26 APR. 2011
ARRIVO

Alla C.A:

Referente Privacy ASL-BA

Bari, lì .....

Oggetto : Regolamento e Modulistica per Videosorveglianza aziendale

Studiodelta, con riferimento alla vs d.d. n. 03 del 03.01.2011, inerente l' affidamento del servizio di consulenza in materia di Privacy, consegna la seguente documentazione:

1. *Regolamento per sistema di Videosorveglianza aziendale*
2. *Documento di attività di videosorveglianza*
3. *Lettera di nomina del Responsabile della videosorveglianza*
4. *Lettera di nomina incaricato videosorveglianza*
5. *Avviso Videosorveglianza per Registrazione*
6. *Avviso Videosorveglianza per Rilevazione*

Si precisa che la su citata documentazione viene consegnata brevi mano all'Avv. Luigi Fruscio dell' Ufficio Privacy ASL-BA, in formato cartaceo e digitale (.doc), editabile per successive eventuali vs modifiche ed integrazioni.

Direzione Tecnica Studiodelta
Timbro e Firma Tecnico
Il Direttore Tecnico
Dr. Nicola Barberini

Studiodelta s.r.l.

Studiodelta S.r.l.
Sede Legale e Operativa
Via G. Amendola, 162/1
Executive Center
70126 Bari (Italy)
Tel [+39] 080.546.18.60
Fax [+39] 080.546.18.78

info@studiodelta.it
www.studiodelta.it

REGOLAMENTO PER SISTEMI DI VIDEOSORVEGLIANZA

Sommario

Art. 1 - Oggetto ed ambito di applicazione

Il presente testo normativo disciplina l'installazione nonché l'uso dei sistemi di videosorveglianza all'interno ed all'esterno delle Strutture dell'Azienda ASL BA.

Art. 2 - Finalità dell'attività di videosorveglianza

L'esercizio dell'attività di videosorveglianza è finalizzato esclusivamente al perseguimento degli obiettivi di protezione degli individui che accedono e sostano nei locali dell'Azienda, di salvaguardia del suo patrimonio mobiliare ed immobiliare. L'attività di cui trattasi è informata anche ad un criterio di gradualità, ovvero avrà intensità diversa a seconda della pericolosità dell'area da sottoporre a controllo.

Art. 3 - Tutela della riservatezza personale

L'attività di videosorveglianza deve essere esercitata nel rispetto delle disposizioni contenute nel D.Lgs. 30 Giugno 2003 n. 196, di seguito denominato "Codice della Privacy".

Le norme di seguito dispiegate garantiscono la conformità delle operazioni inerenti gli impianti visivi ai principi sanciti dal "Provvedimento in materia di videosorveglianza", emanato dall'Autorità Garante per la protezione dei dati personali, in data 8 aprile 2010, di seguito denominato "Provvedimento del Garante". Il presente regolamento assicura, altresì, l'osservanza del diritto di ciascun individuo alla segretezza dell'identità personale ed alla tutela da qualunque forma di abuso dell'immagine.

Art. 4 – Tutela della riservatezza dei lavoratori

In considerazione della necessità di salvaguardare i dipendenti dell'Azienda da forme di controllo del loro operato, l'attività disciplinata dal presente testo viene svolta con attenzione al divieto di controllo a distanza dell'attività lavorativa. Qualora l'installazione degli impianti di cui all'art. 1 venga effettuata in aree nelle quali i dipendenti svolgano la loro prestazione lavorativa o che, comunque, siano abitualmente frequentate dagli stessi, è garantito il rispetto della disposizione dell'art. 4 co. 2 della L. 20 Maggio 1970, n. 300 (Statuto dei Lavoratori).

Art. 5 – Titolare, Responsabili ed Incaricati del trattamento dei dati

Il Titolare del Trattamento dei dati raccolti con i sistemi di videosorveglianza è l'Azienda Sanitaria Locale della Provincia di Bari (ASL BA), nella persona del suo rappresentante legale pro-tempore.

I Responsabili del trattamento sono le persone fisiche che esercitano funzioni direttive nei settori in cui risultano installati i sistemi. Essi sono individuati dal Titolare ed a loro volta designano i soggetti Incaricati del trattamento i quali, a norma dell'art. 30 del Codice della Privacy, operano sotto la diretta autorità dei Responsabili.

Art. 6 – Sicurezza e conservazione dei dati

Gli impianti di videoripresa ed i dati con essi raccolti devono essere salvaguardati, mediante adeguate misure di sicurezza, dai pericoli di distruzione, di perdita e di intrusione da parte di individui non autorizzati ad utilizzarli od a disporne il trattamento. Pur tuttavia la conservazione dei dati può avere un carattere esclusivamente temporaneo ed a tale principio non sono ammesse deroghe. I dati che possano soddisfare le finalità di tutela descritte nell'art. 3, dovranno essere conservati ed eventualmente utilizzati in un lasso di tempo strettamente necessario per conseguire gli scopi per cui sono raccolti, nel rispetto del principio di proporzionalità, ai sensi dell'art. 11 del Codice della Privacy. La conservazione non deve, comunque, superare l'arco temporale delle ventiquattro ore dalla raccolta, fatta salva la necessità di ampliare il suddetto termine, per soddisfare eventuali richieste dell'Autorità Giudiziaria, motivate dalla complessità delle indagini occorrenti ad individuare le modalità ed i responsabili della commissione di un fatto costituente reato.

Art. 7 – Obblighi per i Responsabili della aree videosorvegliate

I Responsabili del trattamento dati delle strutture di questa Azienda, in caso di installazione di impianti di videosorveglianza, dovranno rispettare una serie di obblighi imposti dalla Normativa a tutela della Privacy di seguito riportati :

1- la raccolta e l'uso delle immagini sono consentiti solo se necessari allo svolgimento di funzioni istituzionali e per il perseguimento di finalità di pertinenza dell'Azienda, tra i quali vi sono la sicurezza degli impianti, dei pazienti e degli operatori;
2- i sistemi di videosorveglianza possono riprendere persone identificabili solo se, per raggiungere gli scopi prefissati, non possono essere utilizzati dati anonimi;
3- Tutti coloro che accedono ai locali dell'Azienda devono essere opportunamente informati dell'esistenza di impianti di videosorveglianza nell'area in cui stanno per transitare. L'obbligo di informativa, come disposto dall'art. 13 del "Codice della Privacy", può essere adempiuto anche con una modalità semplificata, ossia con l'esposizione di cartelli indicanti la presenza nell'area di una o più telecamere. I cartelli devono essere collocati in posizione antistante i sistemi di videosorveglianza e devono avere dimensioni e caratteri alfabetici tali da essere chiaramente visibili anche in condizioni di scarsa od insufficiente illuminazione; essi devono anche recare l'indicazione se l'attività è limitata alla sola ripresa o si estende anche alla registrazione delle immagini. L'informativa deve indicare le finalità dell'installazione degli impianti visivi, citate nel precedente art. 2, le modalità di "trattamento dei dati" con essi raccolti, nonché i soggetti che rivestono i ruoli di Titolare e Responsabili del trattamento *(modelli in allegato).*

   Con il termine "dati", ai fini della presente disciplina, si intende l'insieme delle immagini prodotte dai sistemi indicati nell'art. 1.

   Il "trattamento dei dati", ai sensi del disposto del Codice della Privacy, è rappresentato dalle attività che abbiano ad oggetto la raccolta, la registrazione, la conservazione, la visione e la cancellazione dei dati, così come specificati dal comma precedente;

4- al momento dell'istallazione della telecamera occorre valutare se sia realmente necessario raccogliere immagini dettagliate, dove collocare le apparecchiature e la tipologia (fisse o mobili), nel rispetto dei principi di pertinenza e di non eccedenza;
5- va limitata rigorosamente la creazione di banche dati quando è sufficiente installare un sistema a circuito chiuso di sola visione delle immagini senza la loro registrazione;

6- Il controllo eventuale di ambienti sanitari ed il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (ad es. 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 Dlgs 196/03);

7- Il Responsabile della struttura aziendale richiedente l'impianto di videosorveglianza, deve garantire che possano accedere alle immagini solo i soggetti specificamente autorizzati (es. personale medico ed infermieristico) e che le stesse non possano essere visionate da estranei (ad es. 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 (es. rianimazione), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto;

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

9- Nelle strutture aziendali video sorvegliate sarà necessario provvedere alla nomina del Responsabile della videosorveglianza, degli incaricati all'accesso al sistema di videosorveglianza ed alla conservazione del documento sull'attività di videosorveglianza. *(modelli in allegato). Il responsabile della struttura aziendale dovrà richiedere, all'installatore dell'impianto di videosorveglianza, una dichiarazione che attesti la conformità dell'impianto alle misure minime di sicurezza previste dal Dlgs 196/03 e successive prescrizioni. I Responsabili di ciascuna struttura sottoposta a sistema di videosorveglianza dovranno, anche per il tramite di delegati, inviare tutta la documentazione prima citata all'Ufficio Tutela della Privacy - Avv. Luigi Fruscio - in via Lungomare Starita,n.6 a Bari* (referente.privacy@asl.bari.it);

10- Nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa. 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);

11- Ê inammissibile l'installazione di sistemi di videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all'attività lavorativa (ad es. bagni, spogliatoi, docce, armadietti etc..).

12- 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 (ad esempio, per finalità informative / formative e di aggiornamento), possono essere assimilati ai trattamenti temporanei finalizzati alla pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull'attività giornalistica contenute nel Codice della privacy, fermi restando, comunque, i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l'osservanza del codice deontologico per l'attività giornalistica ed il diritto del lavoratore a tutelare la propria immagine opponendosi anche, per motivi legittimi, alla sua diffusione.

Art. 8 – Cancellazione dei dati

In ottemperanza a quanto statuito nella norma che precede, in ordine alla temporaneità della conservazione dei dati, decorso il termine di volta in volta occorrente per stabilire il perseguimento delle finalità indicate nell'art. 2, i dati dovranno essere cancellati con le modalità che saranno ritenute più efficaci, ovvero anche effettuando nuove registrazioni su quelle precedenti, affinché possa essere conseguito l'effetto di rendere non più utilizzabili quelle per le quali è stata decisa l'eliminazione. I Responsabili di ciascuna struttura presso cui sono ubicati i dispositivi di videosorveglianza si renderanno garanti della corretta cancellazione dei dati di cui al presente articolo.

Art. 9 – Inosservanze e provvedimenti conseguenti

La mancata osservanza delle disposizioni contenute nel presente regolamento determinerà l'impossibilità di utilizzare i dati trattati in violazione delle norme regolamentari e legislative, nonché esplicita diffida dal trattare i dati personali.

Art. 10 – Installazione di ulteriori impianti

Qualora si rendesse necessaria l'installazione di ulteriori sistemi di sorveglianza visiva, oltre a quelli già esistenti, le relative operazioni dovranno essere autorizzate dal Titolare del Trattamento, previo parere del Responsabile dell'Ufficio Tutela della Privacy, tramite richiesta scritta, formulata dal Responsabile della Struttura Aziendale in cui gli stessi dovranno essere collocati.

Art. 11 – Norma di rinvio

Per tutti gli aspetti non espressamente disciplinati dalla presente normativa si rinvia al D. Lgs. 30 Giugno 2003 n. 196, al Provvedimento in materia di videosorveglianza, emanato dall'Autorità Garante per la protezione dei dati personali in data 29.04.2004 e 08.04.2010, nonché a tutte le norme di Legge vigenti in materia.

Il Titolare del Trattamento

ASLBA

Lettera di nomina del Responsabile della videosorveglianza

(ai sensi del D.Lgs. 196/03 e del Disciplinare tecnico in materia di misure minime di sicurezza)

Il Titolare del trattamento, [RAGIONE SOCIALE DEL TITOLARE] con sede in [INDIRIZZO] – [CAP, CITTA' E PROVINCIA] – Codice Fiscale e Partita I.V.A. [COD. FISC. E P. IVA] – Tel. [NUMERO DI TELEFONO] – Fax [NUMERO DI FAX] – E-mail: [E-MAIL] nella persona del suo legale rappresentante, ai sensi del D.Lgs. 196/03 (Codice della Privacy) e del Disciplinare tecnico in materia di misure minime di sicurezza, nomina:

[NOME E COGNOME DEL RESPONSABILE DELLA VIDEOSORVEGLIANZA] come Responsabile della videosorveglianza nella seguente UO/Struttura .....

Il Responsabile della videosorveglianza ha il compito di:

- adottare e rispettare le misure di sicurezza indicate e predisposte dal Titolare del trattamento;
- evadere tempestivamente tutte le richieste da parte del Responsabile del trattamento;
- controllare che le telecamere posizionate all'esterno degli edifici siano posizionate in modo da limitare l'angolo di visuale all'area effettivamente da controllare e proteggere. Controllare che le telecamere posizionate all'interno dei locali siano installate esclusivamente in luoghi destinati all'attività lavorativa, fermo restando il divieto di controllo a distanza dei lavoratori;
- adottare le misure necessarie affinché l'accesso ai locali e/o archivi della videosorveglianza sia protetto con una doppia chiave (fisica e/o logica) che ne precluda la visione se non in caso di reale necessità;
- controllare che il periodo di conservazione delle immagini sia limitato a poche ore e comunque non oltre alle 24 ore, salvo casi eccezionali dovuti all'intervento dell'Autorità giudiziaria;
- predisporre un piano di formazione nel caso di nuove assunzioni o cambio di mansione degli Incaricati della videosorveglianza;
- interagire con i Soggetti incaricati di eventuali verifiche, controlli e/o ispezioni;

Il Responsabile della videosorveglianza dichiara di aver preso conoscenza dei compiti che gli sono affidati, di essere a conoscenza di quanto stabilito dal Documento Programmatico sulla Sicurezza, nonché dal D.Lgs. 196/03, e si impegna ad adottare tutte le misure necessarie nell'attuazione delle norme in essi contenute.

[LUOGO], [DATA]

Il Titolare del trattamento

Il Responsabile della videosorveglianza

Commento [EF1]: ***AVVERTENZA***:

I compiti del Responsabile della videosorveglianza sono pedissequamente riportati così come compaiono nel Documento sull'Attività di Videosorveglianza (D.V.A.). Si consiglia, di conseguenza, di modificare il presente documento in armonia e coordinamento con il D.V.A. stesso.

DOCUMENTO SULL'ATTIVITÀ DI VIDEOSORVEGLIANZA

(ai sensi del D.Lgs. 196/03 e del Provvedimento Generale del Garante per la protezione dei dati personali del 29 aprile 2004)

Il Responsabile del Trattamento Dati della U.O./Struttura ..... con sede in [INDIRIZZO] – [CAP, CITTA' E PROVINCIA] — Tel. [NUMERO DI TELEFONO] – Fax [NUMERO DI FAX] – E-mail: [E-MAIL] ai sensi del D.Lgs. 196/03 e del Provvedimento Generale del Garante per la protezione dei dati personali del 29 aprile 2004 e 8 aprile 2010, dichiara quanto segue:

1. che nei locali ove è esercitata l'attività di [DESCRIVERE BREVEMENTE L'ATTIVITA' SVOLTA E/O ESERCITATA] vi è merce della seguente tipologia: [TIPOLOGIA DI MERCE];
2. che pur avendo adottato sistemi di tutela quali [ELENCARE I SISTEMI DI TUTELA] è necessario un sistema di sorveglianza mediante videocamere, che possa garantire un maggiore e più tempestivo controllo degli accessi, in particolare dei seguenti locali [ELENCARE I LOCALI], sia durante gli orari di normale svolgimento dell'attività che, a maggior ragione, durante gli orari di chiusura;
3. che tale sistema è stato individuato mediante il posizionamento di n. [NUMERO DELLE TELECAMERE] videocamere che effettuano [RILEVAZIONE O REGISTRAZIONE] di immagini, senza ingrandimenti o particolari;
4. che tale provvedimento non ha lo scopo di controllare a distanza il Personale dipendente;
5. che tale trattamento rientra tra quelli per cui il Garante per la protezione dei dati personali ha concesso l'esonero dalla richiesta di autorizzazione;
6. che l'installatore ha rilasciato apposita dichiarazione scritta (che si allega in copia) che ne attesta la conformità alle norme in materia;
7. che le immagini videoregistrate, sono conservate presso [LUOGO DI CONSERVAZIONE] per un periodo di [NUMERO ORE] ore e comunque non superiore alle 24 ore, salvo casi eccezionali dovuti all'intervento dell'Autorità giudiziaria;
8. che ha provveduto alla nomina di un Responsabile e degli Incaricati della videosorveglianza;
9. che le immagini verranno trattate nel rispetto delle Leggi;

[LUOGO], [DATA]

Il Responsabile del Trattamento

_____

ASLBA

Lettera di nomina dell'Incaricato della videosorveglianza

(ai sensi del D.Lgs. 196/03 e del Disciplinare tecnico in materia di misure minime di sicurezza)

Il sottoscritto [NOME E COGNOME DEL RESPONSABILE DELLA VIDEOSORVEGLIANZA] in qualità di Responsabile della videosorveglianza e in base a quanto previsto dal Documento Programmatico sulla Sicurezza, nonché dal D.Lgs. 196/03 (Codice della Privacy), nomina:

[NOME E COGNOME DELL'INCARICATO DELLA VIDEOSORVEGLIANZA] come Incaricato della videosorveglianza nella seguente UO/Struttura.....

L'Incaricato della videosorveglianza deve:

- rispettare le direttive impartite dal Responsabile del trattamento;
- utilizzare gli impianti di videosorveglianza esclusivamente per i fini e le modalità indicati nel Documento sull'Attività di Videosorveglianza per la tutela di Persone e/o cose;
- trattare le immagini per le sole finalità per le quali sono state rilevate e/o registrate;
- adottare tutte le misure delle quali si renda necessaria l'adozione immediata ed urgente, al fine della tutela delle immagini, e segnalare tempestivamente l'opportunità di adozione di misure di non immediata applicazione;
- segnalare al Responsabile della videosorveglianza e/o al Responsabile del trattamento eventuali reclami da parte di Terzi, nonché informare gli stessi Responsabili di qualunque fatto che a Suo giudizio possa compromettere la sicurezza delle immagini.

Commento [EF1]: ***AVVERTENZA:***

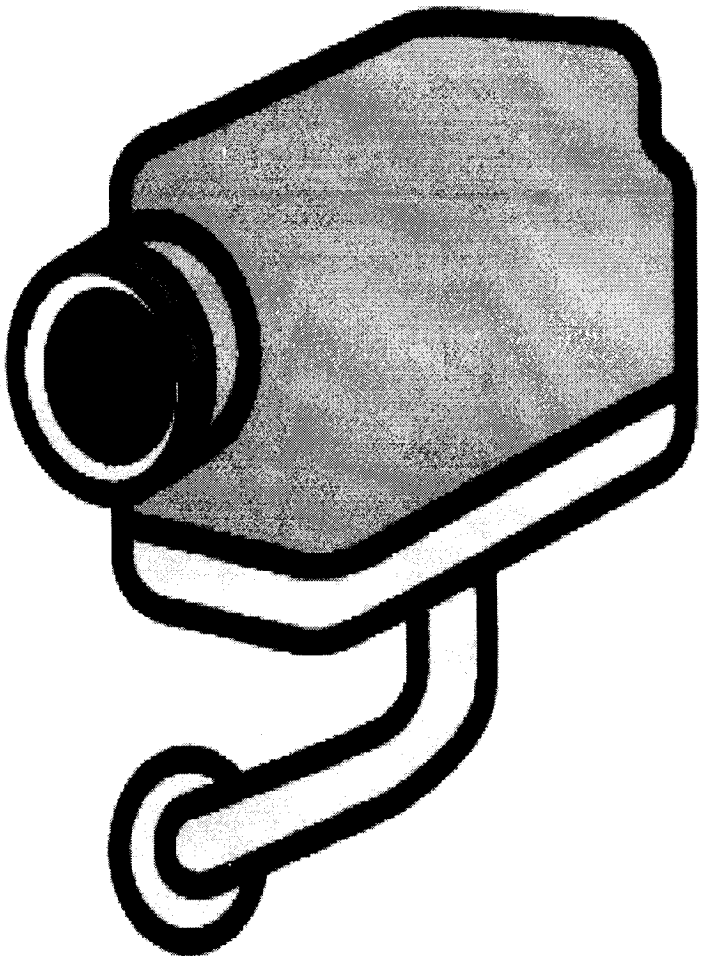
I compiti dell'Incaricato della videosorveglianza sono pedissequamente riportati così come compaiono nel Documento sull'Attività di (D.A.V.). Si consiglia, di conseguenza, di modificare il presente documento in armonia e coordinamento con il D.A.V. stesso.

L'Incaricato della videosorveglianza dichiara di aver preso conoscenza dei compiti che gli sono affidati, di essere a conoscenza di quanto stabilito dal Documento Programmatico sulla Sicurezza, nonché dal D.Lgs. 196/03, e si impegna ad adottare tutte le misure necessarie nell'attuazione delle norme in essi contenute.

[LUOGO], [DATA]

Il Responsabile della videosorveglianza _____

L'Incaricato della videosorveglianza _____



AREA VIDEOSORVEGLIATA

La registrazione è effettuata da

[RAGIONE SOCIALE DEL TITOLARE], per la tutela di Persone e cose

(Art. 13 del D.Lgs. 196/03 e del Disciplinare tecnico in materia di misure minime di sicurezza)

Gentili Utenti,

Il presente locale per ragioni di sicurezza è sorvegliato da sistema di videosorveglianza fissa a mezzo di telecamere.

Le immagini vengono registrate e conservate nel seguente modo: [SPECIFICARE LE MODALITA']

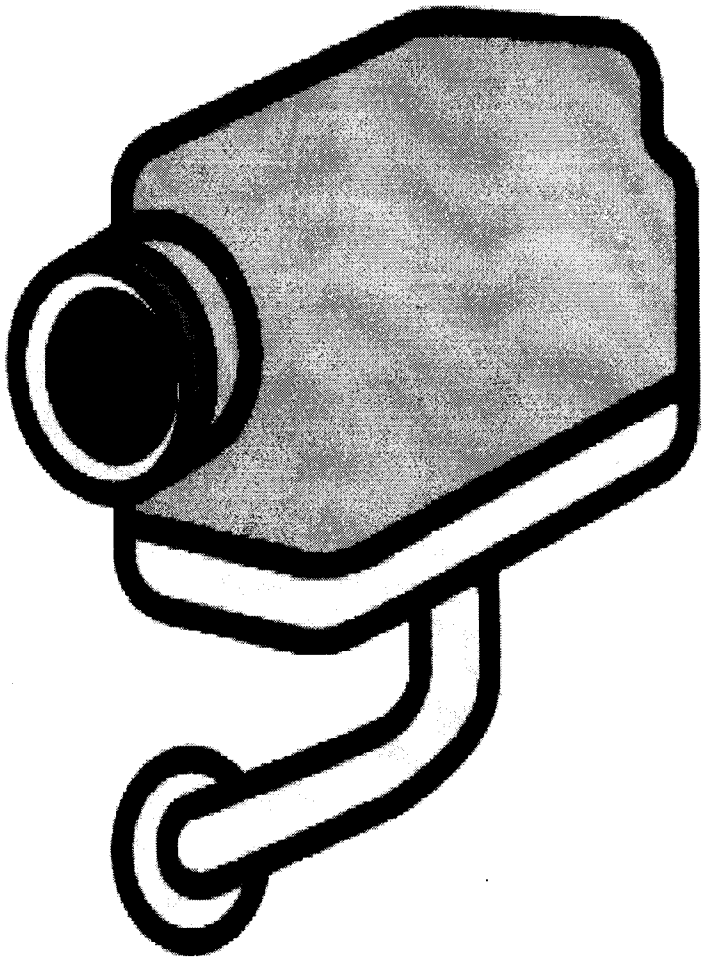
Le immagini sono conservate per 24 ore salve esigenze di giustizia.

L'uso dei sistemi e il trattamento delle immagini è demandato esclusivamente ai Soggetti specificamente incaricati.

Il conferimento dei dati (immagini) non è obbligatorio, ma il divieto di ripresa potrà comportare l'impossibilità di autorizzare l'accesso ai luoghi oggetto di videosorveglianza. Restano ferme le esigenze di controllo e sicurezza anche nell'ambito di indagini investigative.

I soggetti interessati ripresi dalle videocamere possono esercitare i diritti di cui all'art. 7 del D.Lgs. 196/03.

Responsabile del trattamento dei dati è **[NOME E COGNOME DEL RESP.LE DEL TRATTAMENTO]**



AREA VIDEOSORVEGLIATA

La rilevazione è effettuata da

[RAGIONE SOCIALE DEL TITOLARE], per la tutela di Persone e cose

(Art. 13 del D.Lgs. 196/03 e del Disciplinare tecnico in materia di misure minime di sicurezza)

Gentili Utenti,

Il presente locale per ragioni di sicurezza è sorvegliato da sistema di videosorveglianza fissa a mezzo di telecamere.

L'uso dei sistemi e il trattamento delle immagini è demandato esclusivamente ai soggetti specificamente incaricati.

Il conferimento dei dati (immagini) non è obbligatorio, ma il divieto di ripresa potrà comportare l'impossibilità di autorizzare l'accesso ai luoghi oggetto di videosorveglianza.

Restano ferme le esigenze di controllo e sicurezza anche nell'ambito di indagini investigative.

I soggetti interessati ripresi dalle videocamere possono esercitare i diritti di cui all'art. 7 del D.Lgs. 196/03.

Responsabile del trattamento dei dati è **[NOME E COGNOME DEL RESP.LE DEL TRATTAMENTO]**

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Prescrizioni del Garante [art. 154, 1 c) del Codice] - 08 aprile 2010

Bollettino del n. 115/aprile 2010, pag. 0

[doc. web n. 1712680]

vedi anche
[comunicato stampa]
[vademecum]
[provv. 29 aprile 2004]
[Videosorveglianza: il decalogo]

versione grafica (leaflet english version)

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

Sommario

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

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

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

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

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

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

Relatore il prof. Francesco Pizzetti;

1. PREMESSA

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

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

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

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

2. TRATTAMENTO DEI DATI PERSONALI E VIDEOSORVEGLIANZA: PRINCIPI GENERALI

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

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

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

2) protezione della proprietà;

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

4) acquisizione di prove.

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

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

In tale quadro, pertanto, è necessario che:

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

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

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

3. ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI

3.1. Informativa

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

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

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

Il supporto con l'informativa:

- deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non

necessariamente a contatto con gli impianti;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Al predetto trattamento si applicano le prescrizioni contenute nel punto 4.6

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

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

3.2. Prescrizioni specifiche

3.2.1. Verifica preliminare

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

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

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

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

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

3.2.2. Esclusione della verifica preliminare

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

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

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

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

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

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

3.2.3. Notificazione

E' regola generale che i trattamenti di dati personali devono essere notificati al Garante solo se rientrano in casi specificamente previsti (*art. 37 del Codice*). In relazione a quanto stabilito dalla lett. *f*), del comma 1, dell'art. 37,

questa Autorità ha già disposto che non vanno comunque notificati i trattamenti di dati effettuati per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio ancorché relativi a comportamenti illeciti o fraudolenti, quando immagini o suoni raccolti siano conservati temporaneamente(11). Al di fuori di tali precisazioni, il trattamento, che venga effettuato tramite sistemi di videosorveglianza e che sia riconducibile a quanto disposto dall'art. 37 del Codice, deve essere preventivamente notificato a questa Autorità.

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

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

3.3.1. Misure di sicurezza

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

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

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

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

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

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

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

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

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

3.3.2. Responsabili e incaricati

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

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

Il mancato rispetto di quanto previsto nelle lettere da a) ad f) del punto 3.3.1 comporta l'applicazione della sanzione

amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.

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

3.4. Durata dell'eventuale conservazione

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

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

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

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

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

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

3.5. Diritti degli interessati

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

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

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

4. SETTORI SPECIFICI

4.1. Rapporti di lavoro

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

Tali garanzie vanno osservate sia all'interno degli edifici, sia in altri contesti in cui è resa la prestazione di lavoro, come, ad

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

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

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

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

4.2. Ospedali e luoghi di cura

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

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

Il titolare deve garantire che possano accedere alle immagini rilevate per le predette finalità solo i soggetti specificamente autorizzati (es. personale medico ed infermieristico). Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di terzi legittimati (familiari, parenti, conoscenti) di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto o conoscente.

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

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

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

4.3. Istituti scolastici

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

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

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

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

4.4. Sicurezza nel trasporto pubblico

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

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

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

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

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

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

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

4.6. Sistemi integrati di videosorveglianza

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

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

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

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

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

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

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

2) separazione logica delle immagini registrate dai diversi titolari.

Il mancato rispetto delle misure previste ai punti 1) e 2) comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice.

Fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità (v. punto 3.2.1).

5. SOGGETTI PUBBLICI

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

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

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

5.1. Sicurezza urbana

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

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

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

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

5.2. Deposito dei rifiuti

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

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

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

Gli impianti elettronici di rilevamento automatizzato delle infrazioni, utilizzati per documentare la violazione delle disposizioni in materia di circolazione stradale, analogamente all'utilizzo di sistemi di videosorveglianza, comportano un trattamento di dati personali.

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

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

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

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

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

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

f) in considerazione del legittimo interesse dell'intestatario del veicolo di verificare l'autore della violazione e, pertanto, di ottenere dalla competente autorità ogni elemento a tal fine utile, la visione della documentazione video-fotografica deve essere resa disponibile a richiesta del destinatario del verbale; al momento dell'accesso, dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo.

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

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

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

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

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

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

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

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

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

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

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

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

In particolare:

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

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

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

6. PRIVATI ED ENTI PUBBLICI ECONOMICI

6.1. Trattamento di dati personali per fini esclusivamente personali

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

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

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

6.2.1. Consenso

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

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

6.2.2. Bilanciamento degli interessi

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

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

6.2.2.1. Videosorveglianza (con o senza registrazione delle immagini)

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

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

6.2.2.2. Riprese nelle aree condominiali comuni

Qualora i trattamenti siano effettuati dal condominio (anche per il tramite della relativa amministrazione), si evidenzia che tale specifica ipotesi è stata recentemente oggetto di una segnalazione da parte del Garante al

Governo ed al Parlamento(22); ciò in relazione all'assenza di una puntuale disciplina che permetta di risolvere alcuni problemi applicativi evidenziati nell'esperienza di questi ultimi anni. Non è infatti chiaro se l'installazione di sistemi di videosorveglianza possa essere effettuata in base alla sola volontà dei comproprietari, o se rilevi anche la qualità di conduttori. Non è parimenti chiaro quale sia il numero di voti necessario per la deliberazione condominiale in materia (se occorra cioè l'unanimità ovvero una determinata maggioranza).

7. PRESCRIZIONI E SANZIONI

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

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

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

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

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

TUTTO CIÒ PREMESSO IL GARANTE:

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

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

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

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

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

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

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

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

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

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

Roma, 8 aprile 2010

IL PRESIDENTE
F.to Pizzetti

IL RELATORE
F.to Pizzetti

IL SEGRETARIO GENERALE REGGENTE
F.to De Paoli

NOTE

(1). In *www.garanteprivacy.it*; doc. web n. 1003482.

(2). V. l'art. 6, comma 8, del d.l. 23 febbraio 2009, n. 11 convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 23 aprile 2009, n. 38, recante *"Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori"*; d.l. 23 maggio 2008, n. 92, convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 24 luglio 2008, n. 125, recante *"Misure urgenti in materia di sicurezza urbana"*, il cui art. 6 ha novellato l'art. 54 del d.lg. 18 agosto 2000, n. 267, con cui sono stati disciplinati i compiti del sindaco in materia di ordine e sicurezza pubblica. Con il decreto del 5 agosto 2008 il Ministro dell'interno ha stabilito l'ambito di applicazione, individuando la definizione di incolumità pubblica e sicurezza urbana, nonché i correlati ambiti di intervento attribuiti al sindaco. Cfr., altresì, l. 15 luglio 2009, n. 94 recante *"Disposizioni in materia di sicurezza pubblica"* (art. 3).

(3). A tale proposito, va ricordata la l. 24 dicembre 2007, n. 244 recante *"Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2008)"*, il cui art. 1, comma 228, ha previsto, ai fini dell'adozione di misure finalizzate a prevenire il rischio del compimento di atti illeciti da parte di terzi, compresa l'installazione di apparecchi di videosorveglianza, per ciascuno dei periodi d'imposta 2008, 2009 e 2010, la concessione da parte dell'Agenzia delle entrate (*v. d.m. 6 febbraio 2008* recante *"Modalità di attuazione dei commi da 233 a 237, dell'articolo 1, della legge n. 244/2007- credito d'imposta in favore degli esercenti attività di rivendita di generi di monopolio, per le spese sostenute per l'acquisizione e l'installazione di impianti e attrezzature di sicurezza e per favorire la diffusione degli strumenti di pagamento con moneta elettronica, al fine di prevenire il compimento di atti illeciti ai loro danni"*) di un credito d'imposta, determinato nella misura dell'80% del costo sostenuto e, comunque, fino ad un importo massimo di 3.000 euro per ciascun beneficiario, in favore delle piccole e medie imprese commerciali di vendita al dettaglio e all'ingrosso e quelle di somministrazione di alimenti e bevande.

(4). V., a titolo esemplificativo, l.r. Emilia Romagna, 4 dicembre 2003, n. 24 recante "Disciplina della polizia amministrativa locale e promozione di un sistema integrato di sicurezza"; l.r. Friuli Venezia Giulia, 28 dicembre 2007, n. 30 recante "Legge strumentale alla manovra di bilancio (Legge strumentale 2008)"; l.r. Lombardia, 14 aprile 2003, n. 4, recante *"Riordino e riforma della disciplina regionale in materia di polizia locale e sicurezza urbana"*; la l.r. Sicilia, 3 dicembre 2003, n. 20 recante *"Norme finanziarie urgenti e variazioni al bilancio della Regione per l'anno finanziario 2003. Norme di razionalizzazione in materia di organizzazione amministrativa e di sviluppo economico"*.

(5). V., in particolare l'art. 615-bis del codice penale. V. *Provv.* 2 ottobre 2008, doc. *web* n. 1581352.

(6). L. 20 maggio 1970, n. 300

(7). D.l. 24 febbraio 2003, n. 28, convertito, con modificazioni, con l. 24 aprile 2003, n. 88; v. *parere* reso al Ministero dell'interno del 4 maggio 2005, doc. *web* n. 1120732.

(8). D.l. 14 novembre 1992, n. 433, convertito, con modificazioni, dalla legge 14 gennaio 1993, n. 4.

(9). D.lg. 4 febbraio 2000, n. 45.

(10). D.m. 15 settembre 2009 n. 154, recante *"Regolamento recante disposizioni per l'affidamento dei servizi di sicurezza sussidiaria nell'ambito dei porti, delle stazioni ferroviarie e dei relativi mezzi di trasporto e depositi, delle stazioni delle ferrovie metropolitane e dei relativi mezzi di trasporto e depositi, nonché nell'ambito delle linee di trasporto urbano, per il cui espletamento non è richiesto l'esercizio di pubbliche potestà, adottato ai sensi dell'articolo 18, comma 2, del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155"*.

(11). *Provv.* 31 marzo 2004, n. 1/2004 relativo ai casi da sottrarre all'obbligo di notificazione (pubblicato in G.U. 6 aprile 2004, n. 81; doc. *web* n. 852561); v. anche i chiarimenti forniti con nota n. 9654/33365 del 23 aprile 2004 relativamente alla posizione geografica delle persone, doc. *web* n. 993385.

(12). Così stabilito dall'art. 6, comma 8, del d.l. n. 11/2009 cit.

(13). *Provv.* 9 novembre 2005, doc. *web* n. 1191411.

(14). *Provv.* 4 settembre 2009, doc. *web* n. 1651744.

(15). D.l. n. 92/2008 cit.

(16). D.m. 5 agosto 2008 cit.

(17). V. artt. 6 d.l. n. 92/2008 cit., e 6, comma 7, d.l. n. 11/2009 cit.

(18). V. quanto previsto con riferimento al rilevamento a distanza dei limiti di velocità e dei sorpassi vietati dal d.P.R. 16 dicembre 1992, n. 495 recante *"Regolamento di esecuzione e di attuazione del nuovo codice della strada"* (art. 383); circ. Ministero dell'interno del 14 agosto 2009, n. 300/A/10307/09/144/5/20/3 recante *"Direttiva per garantire un'azione coordinata di prevenzione e contrasto dell'eccesso di velocità sulle strade"*; circ. Ministero dell'interno, Dipartimento della pubblica sicurezza, Direzione centrale per la polizia stradale, ferroviaria, delle comunicazioni e per i reparti speciali della Polizia di Stato, del 16 maggio 2008, n. 300/A/1/34197/101/138 riguardante *"Accesso ai documenti amministrativi riguardanti l'attività di accertamento e contestazione delle violazioni in materia di limiti di velocità"* (par. 6); nota del Ministero dell'interno, Dipartimento della pubblica sicurezza, Direzione centrale per la polizia stradale, ferroviaria e delle comunicazioni e per i reparti speciali della Polizia di Stato, prot. n. 300/A/1/38001/144/16/20 del 27 ottobre 2008.

(19). V., ad es., art. 3 d.P.R. 22 giugno 1999, n. 250 recante *"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 L. 15 maggio 1997, n. 127"*.

(20). La disciplina in tema di circolazione stradale prevede che le postazioni di controllo sulla rete stradale per rilevare la velocità debbano essere segnalate preventivamente e rese ben visibili in casi specificatamente delimitati: v., ad es., quanto stabilito in ordine all'utilizzazione dei dispositivi e dei mezzi tecnici di controllo della viabilità finalizzati al rilevamento a distanza dei limiti di velocità, dei sorpassi vietati e delle norme di comportamento sulle autostrade e sulle strade extraurbane principali (artt. 142, 148 e 176 d.lg. 30 aprile 1992, n. 285; art. 4, comma 1, d.lg. 20 giugno 2002, n. 121, conv., con mod., dall'art. 1 l. 1° agosto 2002, n. 168 recante *"Disposizioni urgenti per garantire la sicurezza nella circolazione stradale"*; d.m. 15 agosto 2007 recante *"Attuazione dell'articolo 3, comma 1, lettera b) d.l. 3 agosto 2007, n. 117, recante disposizioni urgenti modificative del codice della strada per incrementare i livelli di sicurezza nella circolazione"*; art. 7 circ. Ministero dell'interno del 14 agosto 2009, n. 300/A/10307/09/144/5/20/3 cit.; circ. Ministero dell'interno 8 aprile 2003, n. 300/A/1/41198/101/3/3/9 *"Direttive per l'utilizzazione e l'installazione dei dispositivi e dei mezzi tecnici di controllo del traffico finalizzati al rilevamento a distanza delle violazioni delle norme di comportamento di cui agli articoli 142 e 148 del d.lg. 30 aprile 1992, n. 285"*).

(21).V. art. 6, comma 8, del d.l. n. 11/2009 cit.

(22). V. segnalazione del Garante del 13 maggio 2008, doc. web n. 1523997.

ALLEGATI

ALLEGATO n. 1

- Per le modalità di utilizzazione del modello, cfr. punto 3.1.
- Se le immagini non sono registrate, sostituire il termine "registrazione" con quello di "rilevazione".

- SCARICA FORMATO JPEG - EPS

ALLEGATO n. 2

- Per le modalità di utilizzazione del modello, cfr. punti 3.1.3 e 4.6, lett. *c*).
- Se le immagini non sono registrate, sostituire il termine "registrazione" con quello di "rilevazione".

- SCARICA FORMATO JPEG - EPS

stampa **chiudi**

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

29 aprile 2004

Bollettino del n. 0/aprile 2004, pag. 0

[doc. web n. 1003482]

[doc. web. n. 1116810]

[v. anche Comunicato stampa]

Videosorveglianza - Provvedimento generale

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.lg. 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 ed 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 uomo ratificata con l. n. 848/1955)*, derivanti da rilevazioni invadenti ed oppressive riguardanti presenze, tracce di passaggi e spostamenti, facilitate dalla crescente interazione dei sistemi via Internet ed 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 e http://europa.eu.int/comm/internal-*

market/privacy/workingroup/wp2004/wpdocs04_en.htm).

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 ed enti pubblici economici (adempimento ad un obbligo di legge, provvedimento del Garante di c.d. "bilanciamento di interessi" o consenso libero ed 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.lg. 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 ed 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 (es., 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 riguardante 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 di 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 ed 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 (es. 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 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 ed 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 es. 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 (es. 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 ed 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 ed 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.lg. 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 es. 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 ed 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 ed 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 es. 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 (es. personale medico ed infermieristico) e che le stesse non possano essere visionate da estranei (ad es. 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 (es. 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 (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)*.

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 ed 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 (per es. 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 ed esclusivamente per svolgere funzioni istituzionali che deve individuare ed 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 ed 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 ED 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 ed enti pubblici economici, la possibilità di raccogliere lecitamente il consenso può risultare, in concreto, fortemente limitata dalle caratteristiche e dalle modalità di funzionamento dei sistemi di rilevazione, i quali riguardano spesso una cerchia non circoscritta di persone che non è agevole o non è possibile contattare prima del trattamento. Ciò anche in relazione a finalità (ad es. di sicurezza o di deterrenza) che non si conciliano con richieste di esplicita accettazione da chi intende accedere a determinati luoghi o usufruire di taluni servizi.

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 ed 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 ed 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 (es., 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 (es. 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, ed espone:

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

IL PRESIDENTE
Rodotà

IL RELATORE
Rasi

IL SEGRETARIO GENERALE
Buttarelli

- Per le modalità di utilizzazione del modello si veda il paragrafo 3.1.
- Se le immagini non sono registrate, sostituire il termine "registrazione" con quello di "rilevazione".

Immagine in formato:

- .EPS
- .JPG
- .GIF

stampa **chiudi**

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimenti a carattere generale - 29 novembre 2000 Bollettino del n. 14/settembre 2000, pag. 28

[doc. web n. 31019]

Videosorveglianza - Il decalogo delle regole per non violare la privacy - 29 novembre 2000

In attesa di una specifica normativa che disciplini l'utilizzo di sistemi di videosorveglianza, il Garante ha ritenuto necessario indicare gli adempimenti, le garanzie e le tutele già oggi necessarie in base ai principi della legge sulla protezione dei dati personali.

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. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti e del dott. Giovanni Buttarelli, segretario generale;

Viste le numerose note pervenute in merito alla conformità alle disposizioni della legge 31 dicembre 1996, n. 675 di alcune iniziative volte ad installare sistemi ed apparecchiature di controllo video;

Visti gli atti d'ufficio e le osservazioni formulate ai sensi dell'art. 15 del regolamento n. 1/2000, adottato con deliberazione n. 15 del 28 giugno 2000 e pubblicano sulla G.U. n. 162 del 13 luglio 2000;

Relatore il prof. Ugo De Siervo;

PREMESSO:

Questa Autorità ha ricevuto numerose richieste in merito alle cautele necessarie per conformare alla legge 31 dicembre 1996, n. 675, gli impianti di videosorveglianza stabili o comunque non occasionali, cioè l'installazione di sistemi, reti ed apparecchiature che permettono la ripresa e l'eventuale registrazione di immagini, in particolare a fini di sicurezza, di tutela del patrimonio, di controllo di determinate aree e di monitoraggio del traffico o degli accessi di veicoli nei centri storici.

Il Garante si è espresso sul tema in diverse occasioni formulando vari pareri e segnalazioni menzionati nella Relazione al Parlamento e al Governo per il 1999, consultabili sul sito *www.garanteprivacy.it* e sul bollettino dell'Autorità "*Cittadini e società dell'informazione*".

La tematica è stata esaminata da questa Autorità per i profili di sua competenza, ovvero per quanto riguarda la liceità e la correttezza del trattamento di dati personali.

In presenza di una crescente utilizzazione di impianti di videosorveglianza da parte di molti soggetti pubblici e privati, il Garante, nell'attesa di una specifica legislazione, reputa necessario sintetizzare gli adempimenti, le garanzie e le tutele già necessari in base alle norme vigenti, per facilitarne la conoscenza da parte degli operatori interessati.

Le regole di base della disciplina sul trattamento dei dati personali, infatti, sono già applicabili alle immagini ed ai suoni, qualora le apparecchiature che li rilevano permettano di identificare, in modo diretto o indiretto, i soggetti interessati.

Chi intende svolgere attività di videosorveglianza deve quindi osservare almeno le seguenti cautele, rispettando comunque il principio di proporzionalità tra mezzi impiegati e fini perseguiti:

1. Tutti gli interessati devono determinare esattamente le finalità perseguite attraverso la videosorveglianza e verificarne la liceità in base alle norme vigenti. Se l'attività è svolta in presenza di un pericolo concreto o per la prevenzione di specifici reati, occorre rispettare le competenze che le leggi assegnano per tali fini solo a determinate amministrazioni pubbliche, prevedendo che alle informazioni raccolte possano accedere solo queste amministrazioni.
2. Il trattamento dei dati deve avvenire secondo correttezza e per scopi determinati, espliciti e legittimi (art. 9, comma 1, lett. a) e b), legge 675/1996).
3. Nei casi in cui la legge impone la notificazione al Garante dei trattamenti di dati personali effettuati da determinati soggetti (art. 7 legge 675/1996), questi devono indicare fra le modalità di trattamento anche la raccolta di informazioni mediante apparecchiature di videosorveglianza. Non è prevista alcuna altra forma di specifica comunicazione o richiesta di autorizzazione al Garante.
4. Si devono fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza, fornendo anche le informazioni necessarie ai sensi dell'art. 10 della legge n. 675/1996. Ciò è tanto più necessario quando le apparecchiature non siano immediatamente visibili.
5. Occorre rispettare scrupolosamente il divieto di controllo a distanza dei lavoratori e le precise garanzie previste al riguardo (art. 4 legge 300/1970).

6. Occorre rispettare i princìpi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando - quando non indispensabili - immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.
7. Occorre determinare con precisione il periodo di eventuale conservazione delle immagini, prima della loro cancellazione, e prevedere la loro conservazione solo in relazione a illeciti che si siano verificati o a indagini delle autorità giudiziarie o di polizia.
8. Occorre designare per iscritto i soggetti - responsabili e incaricati del trattamento dei dati (artt. 8 e 19 della legge 675/1996) - che possono utilizzare gli impianti e prendere visione delle registrazioni, avendo cura che essi accedano ai soli dati personali strettamente necessari e vietando rigorosamente l'accesso di altri soggetti, salvo che si tratti di indagini giudiziarie o di polizia.
9. I dati raccolti per determinati fini (ad esempio, ragioni di sicurezza, tutela del patrimonio) non possono essere utilizzati per finalità diverse o ulteriori (ad esempio, pubblicità, analisi dei comportamenti di consumo), salvo le esigenze di polizia o di giustizia, e non possono essere diffusi o comunicati a terzi.
10. I particolari impianti per la rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato devono essere conformi anche alle disposizioni contenute nel d.P.R. 250/1999. E' altresì necessario che la relativa documentazione sia conservata per il solo periodo necessario per contestare le infrazioni e definire il relativo contenzioso e che ad essa si possa inoltre accedere solo a fini di indagine giudiziaria o di polizia.

Per gli impianti di videosorveglianza finalizzati esclusivamente alla sicurezza individuale (ad esempio, il controllo dell'accesso alla propria abitazione) si ricorda che questi non rientrano nell'ambito dell'applicazione della legge 675/1996, ricorrendo le condizioni di cui all'art. 3. Occorre, però, che le riprese siano strettamente limitate allo spazio antistante tali accessi, senza forme di videosorveglianza su aree circostanti e senza limitazioni delle libertà altrui. Occorre inoltre che le informazioni raccolte non siano in alcun modo comunicate o diffuse. Altrimenti si rientra nell'ambito di applicazione generale della legge 675/1996 e devono, quindi, essere rispettate tutte le indicazioni di cui ai punti precedenti.

TUTTO CIÒ PREMESSO IL GARANTE:

segnala ai titolari del trattamento interessati, ai sensi dell'art. 31, comma 1, lett. c), della legge n. 675/1996, la necessità di conformare il trattamento dei dati ai principi della legge n. 675/1996 richiamati nel presente provvedimento.

Roma, 29 novembre 2000

IL PRESIDENTE
Rodotà

IL RELATORE
De Siervo

IL SEGRETARIO GENERALE
Buttarelli

stampa **chiudi**

SISTEMI DI VIDEOSORVEGLIANZA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

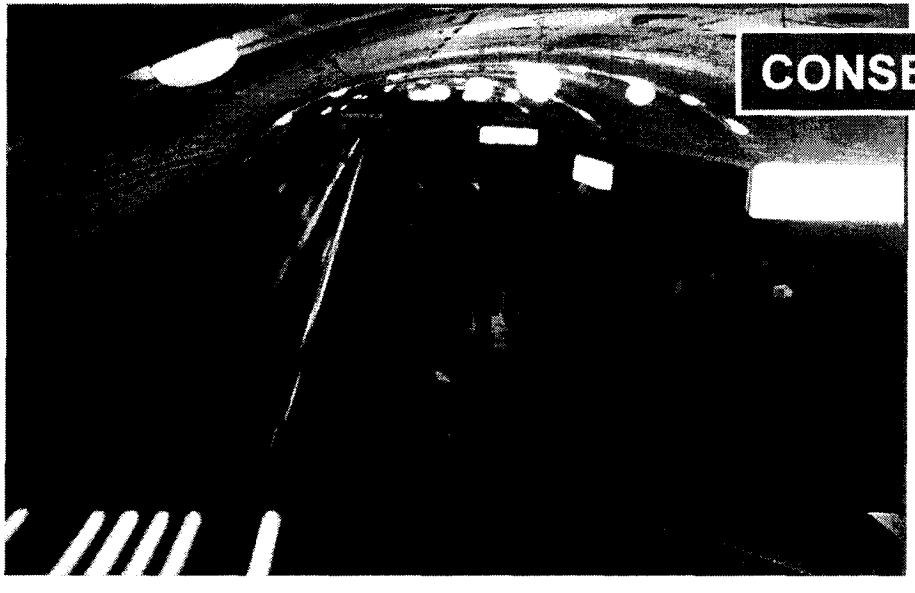
Il nuovo provvedimento generale, che sostituisce quello emanato nel 2004, introduce importanti novità in considerazione:

- **dell'aumento massiccio di sistemi di videosorveglianza per diverse finalità (prevenzione accertamento e repressione dei reati, sicurezza pubblica, tutela della proprietà privata, controllo stradale etc.)**
- **dei numerosi interventi legislativi adottati in materia: tra questi, quelli più recenti che hanno attribuito ai sindaci e ai comuni specifiche competenze, in particolare in materia di sicurezza urbana, così come le norme, anche regionali, che hanno incentivato l'uso di telecamere.**

PRINCIPI GENERALI

INFORMATIVA

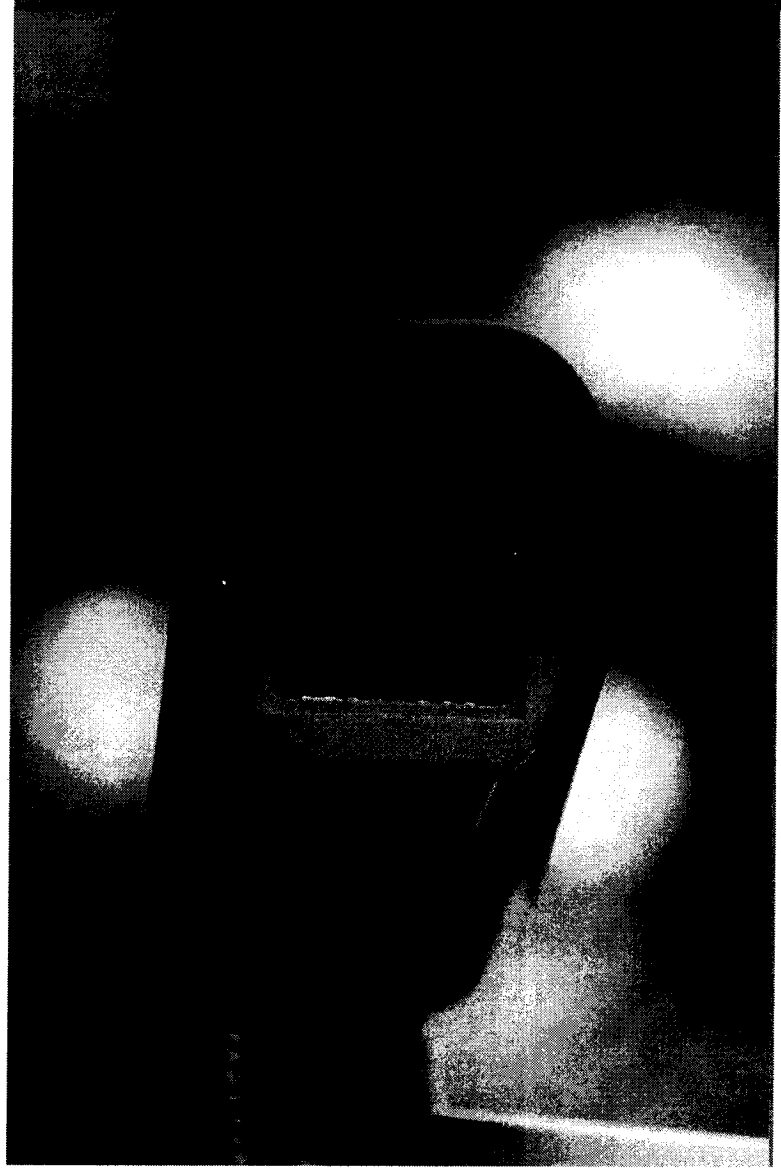
- I cittadini che transitano in aree sorvegliate devono essere **informati con cartelli**, visibili al buio se il sistema di videosorveglianza è attivo in orario notturno.
- I sistemi di videosorveglianza installati da soggetti pubblici e privati (esercizi commerciali, banche, aziende etc.) **collegati alle forze di polizia** richiedono uno **specifico cartello informativo**, sulla base del modello elaborato dal Garante.
- Le telecamere istallate a **fini di tutela dell'ordine e della sicurezza pubblica** non devono essere segnalate, ma il Garante auspica l'utilizzo di cartelli che informino i cittadini.



CONSERVAZIONE

- Le immagini registrate possono essere **conservate** per **periodo limitato** e fino ad un **massimo di 24 ore**, fatte salve **speciali esigenze di ulteriore conservazione** in relazione a indagini di polizia e giudiziarie.
- Per **attività particolarmente rischiose** (es. banche) è ammesso un tempo più ampio, che **non può superare** comunque la **settimana**.
- Eventuali esigenze di allungamento della conservazone devono essere sottoposte a **verifica preliminare** del Garante.

SETTORI DI PARTICOLARE INTERESSE



- **Sicurezza urbana:** i **Comuni** che installano telecamere per fini di sicurezza urbana hanno l'*obbligo di mettere cartelli* che ne segnalino la presenza, salvo che le attività di videosorveglianza siano riconducibili a tutela della sicurezza pubblica, prevenzione, accertamento o repressione dei reati. La conservazione dei dati non può superare i 7 giorni, fatte salve speciali esigenze.
- **Sistemi integrati:** per i sistemi che collegano telecamere tra soggetti diversi, sia pubblici che privati, o che consentono la fornitura di servizi di videosorveglianza "in remoto" da parte di società specializzate (*es.* società di vigilanza, *Internet providers*) mediante collegamento telematico ad un unico centro, sono obbligatorie specifiche misure di sicurezza (*es.* contro accessi abusivi alle immagini). Per alcuni sistemi è comunque necessaria la *verifica preliminare* del Garante.
- **Sistemi intelligenti:** per i sistemi dotati di *software* che permettono l'associazione di immagini a dati biometrici (es. "riconoscimento facciale") o in grado, ad esempio, di riprendere e registrare automaticamente comportamenti o eventi anomali e segnalarli (es. *motion detection*) è obbligatoria la *verifica preliminare* del Garante.
- **Violazioni al codice della strada:** obbligatori i cartelli che segnalano sistemi elettronici di rilevamento delle infrazioni. Le telecamere devono riprendere solo la targa del veicolo (non quindi conducente, passeggeri, eventuali pedoni). Le fotografie o i video che attestano l'infrazione non devono essere inviati al domicilio dell'intestatario del veicolo.
- **Deposito rifiuti:** lecito l'utilizzo di telecamere per controllare discariche di sostanze pericolose ed "eco piazzole", per monitorare modalità del loro uso, tipologia dei rifiuti scaricati e orario di deposito.

SETTORI SPECIFICI

- **Luoghi di lavoro:** le telecamere possono essere installate solo nel rispetto delle *norme in materia di lavoro*. Vietato comunque il *controllo a distanza* dei lavoratori, sia all'interno degli edifici, sia in altri luoghi di prestazione del lavoro (es. cantieri, veicoli).
- **Ospedali e luoghi di cura:** no alla diffusione di immagini di persone malate mediante *monitor* quando questi sono collocati in locali accessibili al pubblico. E' ammesso, nei casi indispensabili, il *monitoraggio* da parte del personale sanitario dei pazienti ricoverati in particolari reparti (*es.* rianimazione), ma l'accesso alle immagini deve essere consentito solo al personale autorizzato e ai familiari dei ricoverati.
- **Istituti scolastici**: ammessa l'installazione di sistemi di videosorveglianza per la *tutela contro gli atti vandalici*, con riprese delimitate alle sole aree interessate e solo negli orari di chiusura.
- **Taxi:** le telecamere non devono riprendere in modo stabile la *postazione di guida* e la loro presenza deve essere segnalata con appositi contrassegni.
- **Trasporto pubblico:** lecita l'installazione su mezzi di trasporto pubblico e presso le fermate, ma rispettando limiti precisi (*es.* angolo visuale circoscritto, riprese senza l'uso di *zoom*).
- **Web cam a scopo turistico:** la ripresa delle immagini deve avvenire con modalità che non rendano identificabili le persone.
- **Tutela delle persone e della proprietà:** contro possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, prevenzione incendi, sicurezza del lavoro ecc., si possono installare telecamere *senza il consenso dei soggetti ripresi*, ma sempre sulla base delle prescrizioni indicate dal Garante.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Per un quadro completo sul corretto impiego dei sistemi di videosorveglianza, è possibile:

consultare il **sito Internet del Garante per la protezione dei dati personali** http://www.garanteprivacy.it che, nell'**indice per materia**, ospita una sezione dedicata al tema **videosorveglianza**

oppure

contattare l'**URP del Garante:** urp@garanteprivacy.it
