

Videosorveglianza - Provvedimento generale sulla videosorveglianza

[doc. web n. 1003482]

Sommario

1. Premessa

2. Principi generali

- 2.1. Principio di liceità
- 2.2. Principio di necessità
- 2.3. Principio di proporzionalità
- 2.4. Principio di finalità

3. Adempimenti

- 3.1. Informativa
- 3.2. Prescrizioni specifiche
 - 3.2.1. Verifica preliminare
 - 3.2.2. Autorizzazioni
 - 3.2.3. Altri esami preventivi
 - 3.2.4. Notificazione
- 3.3. Soggetti preposti e misure di sicurezza
 - 3.3.1. Responsabili e incaricati
 - 3.3.2. Misure di sicurezza
- 3.4. Durata dell'eventuale conservazione
- 3.5. Documentazione delle scelte
- 3.6. Diritti degli interessati

4. Settori specifici

- 4.1. Rapporti di lavoro
- 4.2. Ospedali e luoghi di cura
- 4.3. Istituti scolastici
- 4.4. Luoghi di culto e di sepoltura

5. Soggetti pubblici

- 5.1. Svolgimento di funzioni istituzionali
- 5.2. Informativa
- 5.3. Accessi a centri storici
- 5.4. Sicurezza nel trasporto urbano
- 5.5. Deposito dei rifiuti

6. Privati ed enti pubblici economici

- 6.1. Consenso
- 6.2. Bilanciamento degli interessi
 - 6.2.1. Profili generali
 - 6.2.2. Registrazione delle immagini
 - 6.2.3. Videosorveglianza senza registrazione
 - 6.2.4. Videocitofoni
 - 6.2.5. Riprese nelle aree comuni

7. Prescrizioni e sanzioni

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'adeguata 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/workinggroup/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 imminente, 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 evidenzia 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 condomini 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".