



Prefettura - Ufficio territoriale del Governo di Cremona

Prot. nr. 28793/A1/O.S.P.
Allegati: uno

Cremona, 20 ottobre 2010

**LA PRESENTE CIRCOLARE NON
VERRÀ INVIATA TRAMITE POSTA**

AI SIGG. SINDACI DEI COMUNI DELLA
PROVINCIA **LORO SEDI**

e, p.c. AL SIG. PRESIDENTE DELLA PROVINCIA
di **CREMONA**

AL SIG. QUESTORE
di **CREMONA**

AL SIG. COMANDANTE PROVINCIALE DEI
CARABINIERI di **CREMONA**

AL SIG. COMANDANTE PROVINCIALE DELLA
GUARDIA DI FINANZA
di **CREMONA**

AL SIG. COMANDANTE PROVINCIALE DEL
CORPO FORESTALE DELLO STATO
di **CREMONA**

OGGETTO: Sistemi di videosorveglianza.

Faccio seguito alla riunione del Comitato Provinciale per l'Ordine e la Sicurezza Pubblica, tenuta il giorno 14 ottobre u.s., cui sono state invitate le SS.LL., in occasione della quale è stata richiamata l'attenzione sulla proficuità e sulla funzionalità del sistema di videosorveglianza, quale mezzo di prevenzione e repressione del crimine nonché di controllo a distanza del territorio.

In particolare, anche alla luce della circolare del Ministero dell'Interno, sono state evidenziate le nuove regole con le quali il Garante della privacy ha rivisto le disposizioni in materia di sistemi di videosorveglianza, aggiornandole alla luce delle nuove norme che hanno attribuito ai sindaci ed ai comuni specifiche competenze in materia di "sicurezza urbana".

Al riguardo, il medesimo Dicastero ha osservato che le linee guida definite in materia – peraltro trasmesse alla SS.LL. con circolare prefettizia n. 2731/12B-2B/A1 in data 10 ottobre 2005, reperibile sul sito <http://sito.rup.cr.it/prefettura-utg.cremona> - per le parti



Prefettura - Ufficio territoriale del Governo di Cremona

non interessate dalle nuove norme, rimangono un indiscusso caposaldo del sistema, in particolare per ciò che attiene alla fondamentale distinzione tra sicurezza primaria e secondaria.

Le nuove regole diramate dal Garante contengono un apposito capitolo che disciplina le modalità di attivazione dei sistemi di videosorveglianza per la tutela della "sicurezza urbana", nonché i termini di conservazione dei dati registrati.

Il medesimo Ministero ha, inoltre, rilevato come l'utilizzazione dei sistemi di videosorveglianza per il controllo di luoghi pubblici o aperti al pubblico, qualora si profilino aspetti di tutela dell'ordine e della sicurezza pubblica, oltre a quelli di sicurezza urbana, possa determinare l'attrazione di dette apparecchiature nell'ambito delle previsioni di cui al punto 3.1.1 del citato provvedimento del Garante, con conseguente applicazione dell'art. 53 del Codice in materia di protezione dei dati personali e relativo affievolimento di alcuni principi di garanzia, quali, in particolare, quello dell'informativa di cui all'art. 13 del cennato Codice.

Nel richiamare, pertanto, le considerazioni svolte nel corso della cennata riunione del Comitato Provinciale per l'Ordine e la Sicurezza Pubblica, ritengo utile trasmettere una sintesi - elaborata e presentata in detta occasione dal relatore, dott. Gerardo Acquaviva, Vice Questore Vicario - del provvedimento del Garante, il cui testo è stato integralmente pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana n. 99 del 29 aprile 2010.

Quanto sopra quale contributo per le SS.LL. al fine di assecondare la puntuale applicazione della norme in argomento, che contempererà l'esigenza di assicurare le più favorevoli condizioni di sicurezza urbana con il rispetto del principio generale di protezione dei dati personali.

Resto in attesa di ricevere notizie concernenti le eventuali iniziative intraprese o le problematiche rilevate nel delineato settore.

IL PREFETTO
(Bruno di Clarafond)

smt/EG

**Provvedimento generale del Garante per la protezione dei dati personali
in materia di videosorveglianza**

Provvedimento generale 8 aprile 2010	Il Provvedimento generale, che sostituisce quello del 29 aprile 2004, si è reso necessario sia per il sempre più frequente ricorso ai sistemi di videosorveglianza sia in ragione dei numerosi interventi legislativi adottati in materia, e, in particolare, quelli più recenti che hanno attribuito ai sindaci e ai comuni specifiche competenze in materia di sicurezza urbana.
Profilo generale	<ul style="list-style-type: none"> ➤ I sistemi integrati di videosorveglianza possono essere adottati solo nel rispetto di specifiche garanzie per la libertà delle persone. ➤ Obbligo di informativa mediante apposizione di nuovi cartelli (anche luminosi) per segnalare la presenza di telecamere collegate con le sale operative delle F. P.. ➤ Obbligo di sottoporre alla verifica del Garante della privacy, prima della loro attivazione, i sistemi che presentino rischi per i diritti e le libertà fondamentali delle persone, come i sistemi tecnologicamente avanzati (es. dati biometrici) o «intelligenti» (in grado di rilevare automaticamente comportamenti anomali), ovvero la necessità di prolungare la conservazione delle immagini oltre il termine previsto (una settimana per le F.P.).
Profili di interesse per le Forze di Polizia	Il Provvedimento non va ad incidere sulle attività di videosorveglianza effettuate dalle F. P. per finalità di tutela dell'ordine e della sicurezza pubblica, salvaguardando, nel contempo, il trattamento e la conservazione dei dati per esigenze investigative, richiamando espressamente le deroghe previste dall'art. 53 del Codice in materia di protezione dei dati personali.
Informativa	I cittadini che transitano nelle aree sorvegliate devono essere informati con cartelli della presenza delle telecamere, i cartelli devono essere resi visibili anche quando il sistema di videosorveglianza è attivo in orario notturno. Nel caso in cui i sistemi di videosorveglianza installati da soggetti pubblici e privati siano collegati alle F. P. è necessario apporre uno specifico cartello, sulla base del modello elaborato dal Garante. Le telecamere installate a fini di tutela dell'ordine e della sicurezza pubblica non devono essere segnalate, ma il Garante auspica comunque l'utilizzo di cartelli che informino i cittadini.
Conservazione dei dati	Le immagini registrate possono essere conservate per un periodo limitato e fino ad un massimo di 24 ore, fatte salve speciali esigenze di ulteriore conservazione in relazione a indagini. Per attività particolarmente rischiose (esempio le banche) è ammesso un tempo più ampio, che non può superare comunque la settimana. Eventuali esigenze di ulteriore prolungamento dovranno essere sottoposte a verifica preliminare del Garante.
Sicurezza Urbana	I Comuni che installano telecamere per fini di sicurezza urbana hanno l'obbligo di mettere cartelli che ne segnalino la presenza, salvo che le attività di videosorveglianza siano riconducibili a quelle di tutela specifica della sicurezza pubblica, prevenzione, accertamento o repressione dei reati. 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 (società di vigilanza, Internet providers) mediante collegamento telematico ad un unico centro, sono obbligatorie specifiche misure di sicurezza. Per alcuni sistemi è necessaria la verifica preliminare del Garante.
Sistemi intelligenti	Per i sistemi di videosorveglianza «intelligenti» dotati di software che permettono l'associazione di immagini a dati biometrici (come il «riconoscimento facciale») o in grado, ad esempio, di riprendere e registrare automaticamente comportamenti o eventi anomali e segnalarli («motion detection») è obbligatoria la verifica preliminare del Garante.
Violazioni al Codice della strada	Sono obbligatori i cartelli che segnalino i sistemi elettronici di rilevamento delle infrazioni. Le telecamere devono riprendere solo la targa del veicolo (non quindi conducente, passeggeri, eventuali pedoni). Le fotografie/ video attestanti l'infrazione non devono essere inviati al domicilio dell'intestatario del veicolo.
Deposito rifiuti	E' lecito l'utilizzo di telecamere per controllare discariche di sostanze pericolose, per monitorare il loro uso, la tipologia dei rifiuti scaricati e l'orario di deposito.
Luoghi di lavoro	Le telecamere possono essere installate solo nel rispetto delle norme in materia di lavoro. E' vietato comunque il controllo a distanza dei lavoratori, sia all'interno degli edifici sia in altri luoghi di lavoro.
Ospedali e luoghi di cura	Non è consentita la diffusione di immagini di persone malate mediante monitor quando questi sono collocati in locali accessibili al pubblico. È ammesso, nei casi indispensabili, il monitoraggio da parte del personale sanitario dei pazienti ricoverati in particolari reparti (ad esempio, in rianimazione), ma l'accesso alle immagini deve essere consentito solo al personale autorizzato e ai familiari dei ricoverati.
Istituti scolastici	E' ammessa l'installazione di sistemi di videosorveglianza per la tutela dagli atti vandalici, con riprese delimitate alle sole aree interessate e solo negli orari di chiusura.
Trasporto pubblico e Taxi	E' 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). TAXI: le telecamere non devono riprendere in modo stabile la postazione di guida.
Web cam a scopo turistico	La ripresa delle immagini deve avvenire con modalità che non rendano identificabili le persone.
Soggetti privati	A tutela delle persone e della proprietà, contro possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, prevenzione incendi, sicurezza del lavoro, si possono installare telecamere senza il consenso dei soggetti ripresi, ma sempre sulla base delle prescrizioni indicate dal Garante.

Oggetto: Provvedimento in materia di videosorveglianza - 8 aprile 2010.

Sintesi.

Premessa

Il trattamento dei dati personali effettuato mediante l'uso dei sistemi di videosorveglianza non forma oggetto di legislazione specifica in quanto, al riguardo, si applicano le disposizioni generali in tema di protezione dei dati personali. Il Garante per la protezione dei dati personali, in considerazione dei numerosi interventi legislativi in materia e dell'ingente quantità di quesiti, segnalazioni e reclami ha ritenuto necessario intervenire in materia di videosorveglianza con un nuovo provvedimento generale, emanato in data 8 aprile 2010, che sostituisce quello del 29 aprile 2004. Tra l'altro, nel quinquennio di relativa applicazione, talune disposizioni di legge hanno attribuito ai sindaci e ai comuni specifiche competenze volte a garantire l'incolumità pubblica e la sicurezza urbana, mentre altre norme, statali e regionali 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.

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 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, sul controllo a distanza dei lavoratori, in materia di sicurezza presso stadi e impianti sportivi, o con riferimento a musei, biblioteche statali e archivi di Stato, in relazione ad impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali e, ancora, nell'ambito dei porti, delle stazioni ferroviarie, delle stazioni delle ferrovie metropolitane e nell'ambito delle linee di trasporto urbano.

In tale quadro, pertanto, è necessario che:

- a) il trattamento dei dati attraverso sistemi di videosorveglianza sia fondato su uno dei presupposti di *liceità* che il Codice prevede espressamente per i soggetti pubblici 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);
- 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*).

Adempimenti applicabili a soggetti pubblici e privati.

Informativa

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorveglianza; 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 e riportato in *fac-simile* nell'[allegato n. 1](#). 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.

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.

L'obbligo di fornire una preventiva informativa agli interessati, non è applicabile 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 confluirci 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.

Tuttavia, 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 ostanto in concreto specifiche ragioni di tutela e sicurezza pubblica o di prevenzione, accertamento o repressione dei reati. 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.

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).

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, è possibile utilizzare il modello semplificato di informativa "minima" - indicante il titolare del trattamento, la finalità perseguita ed il collegamento con le forze di polizia riportato in *fac-simile* nell'[allegato n. 2](#). Nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati, tale collegamento deve essere reso noto.

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.

Prescrizioni specifiche – La verifica preliminare.

I trattamenti di dati personali nell'ambito di una attività di videosorveglianza devono essere effettuati rispettando le misure e gli accorgimenti prescritti dal Garante 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 del Garante 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*). In linea generale l'utilizzo di sistemi integrati di videosorveglianza deve essere sottoposto a verifica preliminare. 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; 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 all'Autorità del Garante.

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

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, l'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.

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

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 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;
- 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*).

Il mancato rispetto di quanto previsto nelle lettere da a) ad f) 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.

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 (art.6, co.8, del D.L. n. 11/2009), il termine massimo di durata della conservazione dei dati è limitato *"ai sette giorni successivi alla*

rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione".

In tutti i casi in cui si voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, una richiesta in tal senso deve essere sottoposta ad una **verifica preliminare** del Garante e comunque essere ipotizzata 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.

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*).

SETTORI SPECIFICI

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; 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).

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.

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. Inoltre, devono essere adottati tutti gli ulteriori accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate, in armonia con l'art. 83 del Codice. 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.

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. 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. 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.

Sicurezza nel trasporto pubblico

Alcune situazioni di particolare rischio possono fare ritenere lecita l'installazione di sistemi di videosorveglianza sia su mezzi di trasporto pubblici, sia presso le fermate dei predetti mezzi. 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. 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](#) e indicanti, comunque, il titolare del trattamento, nonché la finalità perseguita. 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.

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 in tema di videosorveglianza presso le aree di fermata, comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-ter, del Codice.

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.

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](#). Tale collegamento deve essere altresì reso noto nell'ambito del testo completo di informativa reso eventualmente disponibile agli interessati .

Le modalità di trattamento sopra elencate richiedono l'adozione di specifiche misure di sicurezza ulteriori rispetto a quelle precedentemente individuate, 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 all'Autorità.

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](#).

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 (D.l. n.92/2008). Al fine di prevenire e contrastare determinati pericoli (D.m.5 agosto 2008) 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.

Non spetta al relatore 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.

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.

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).

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. 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, 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 (art.3 D.P.R.22 giugno 1999,n.250), 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 videofotografica 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.

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.

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'ideale 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. 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*).

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. L'Autorità ha già individuato un quadro di specifiche garanzie in ordine alle corrette modalità che vengono qui ulteriormente richiamate.

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 ai 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.

PRIVATI ED ENTI PUBBLICI ECONOMICI

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

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'ideale alternativa nell'ambito dei requisiti equipollenti del consenso di cui all'art. 24, comma 1, del Codice.

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.

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.).

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; 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 provvedimento. 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*).

Inoltre il Garante

1. prescrive ai titolari del trattamento di dati personali effettuato tramite sistemi di videosorveglianza, di adottare le misure e gli accorgimenti già illustrati 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**;

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

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

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.

ALLEGATO n. 1

- Se le immagini non sono registrate, sostituire il termine "registrazione" con quello di "rilevazione".



ALLEGATO n. 2

- Se le immagini non sono registrate, sostituire il termine "registrazione" con quello di "rilevazione".

