PROVINCIA DI BRESCIA

Allegato A al "REGOLAMENTO DELLA POLIZIA PROVINCIALE PER LA DISCIPLINA DELLA VIDEOSORVEGLIANZA"

Allegato Tecnico

Il presente documento contiene gli aspetti tecnici e di dettaglio della disciplina dettata dal "Regolamento della Polizia Provinciale per la disciplina della videosorveglianza" e riporta, in appendice, il Provvedimento in materia di videosorveglianza emanato dal Garante per la Protezione dei Dati Personali in data 8 aprile 2010 nonché le FAQ emanate nell'anno 2020, i cui contenuti si intendono qui integralmente recepiti.
I sistema di videosorveglianza prevede esclusivamente il trattamento di dati personali rilevati mediante le riprese foto e video e che, in relazione ai luoghi di installazione delle videocamere, interessano i soggetti ed i veicoli che transiteranno nell'area interessata.

1 – Sala di controllo e personale autorizzato

L'infrastruttura che gestisce i sistemi di videosorveglianza (sulla quale sono memorizzate le foto e le riprese video raccolte dai vari dispositivi installati sul territorio) è dislocata in appositi locali (sala di controllo o server farm).
I locali sono separati dai normali uffici e l'accesso è monitorato (gli accessi sono registrati su apposito registro ovvero identificati da chiavi univoche di accesso; i locali sono inoltre provvisti di un sistema interno di videosorveglianza per la registrazione delle immagini all'interno dei locali della server farm).
L'accesso alla sala controllo è consentito solamente agli amministratori di sistema, al personale in servizio del Corpo di Polizia Provinciale autorizzato dal Comandante e agli incaricati addetti ai servizi, di cui ai successivi punti. In particolare, è consentito l'accesso ai tecnici della ditta installatrice degli impianti di videosorveglianza e che svolge il servizio di manutenzione degli impianti stessi, previa nomina a responsabile esterno del trattamento dei dati; l'accesso alla server farm sarà consentito limitatamente per lo svolgimento dei necessari interventi di manutenzione che non potranno essere svolti da remoto.
Possono essere autorizzati all'accesso alla sala controllo solo incaricati di servizi rientranti nei compiti istituzionali dell'ente di appartenenza e per scopi connessi alle finalità di cui al presente regolamento, nonché il personale addetto alla manutenzione degli impianti, i cui nominativi dovranno essere comunicati per iscritto al Comandante della Polizia Provinciale. Il Comandante, qualora lo ritenesse necessario per lo svolgimento del servizio di manutenzione, potrà richiedere, al Settore della Innovazione, il rilascio di una chiave di accesso fisico ai locali da assegnare al fornitore che svolge il servizio di manutenzione.
Il Responsabile del trattamento impartisce idonee istruzioni atte ad evitare assunzioni o rilevamento di dati da parte delle persone autorizzate all'accesso per le operazioni di manutenzione degli impianti e di pulizia dei locali.
Gli incaricati dei servizi di cui al presente regolamento vigilano sul puntuale rispetto delle istruzioni e sulla corretta assunzione di dati pertinenti e non eccedenti rispetto allo scopo per cui è stato autorizzato l'accesso.

I sistemi di controllo fisico degli accessi ai locali ove sono situati gli apparati di archiviazione dei flussi video del sistema di videosorveglianza della Provincia di Brescia (sala di controllo) e quelli di controllo logico ai sistemi software di gestione delle immagini devono essere dotati di una funzionalità di tracciamento degli accessi (log) che consentono al Responsabile interno del trattamento dei dati di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa. I "log" di accesso alle funzionalità software dovranno essere conservati per la durata di anni cinque.

2 – Nomina dei soggetti autorizzati alla gestione dell'impianto di videosorveglianza

Il Responsabile designa e nomina i soggetti autorizzati in numero sufficiente a garantire la gestione del servizio di videosorveglianza.

I soggetti di cui sopra sono nominati tra il personale della Polizia Provinciale di Brescia, gli Ufficiali ed Agenti operativi del Corpo della Polizia Provinciale che per esperienza, capacità ed affidabilità forniscono idonea garanzia nel pieno rispetto delle vigenti disposizioni in materia di trattamento e sicurezza dei dati.

La gestione dell'impianto di videosorveglianza è riservata al Corpo di Polizia Provinciale. Con l'atto di nomina, saranno affidati i compiti specifici e le puntuali prescrizioni per l'utilizzo dei sistemi. In particolare, i compiti affidati agli incaricati, nello specifico, sono quelli di:

a) trattare tutti i dati personali di cui vengono a conoscenza nell'ambito dello svolgimento delle funzioni in modo lecito e secondo correttezza;
b) accedere ai dati unicamente con le credenziali assegnate senza che queste vengano comunicate a soggetti terzi non autorizzati; le credenziali dovranno essere modificate con cadenza trimestrale ed essere composte da minimo otto caratteri alfanumerici comprensivi di un carattere speciale; le credenziali non dovranno fare alcun riferimento al soggetto assegnatario non dovendo contenere elementi personali riconducibili al medesimo;
c) effettuare la sola consultazione esclusivamente per lo svolgimento delle proprie mansioni;
d) verificare che le registrazioni non superino i termini temporali di legge;
e) comunicare al Comandante della Polizia Provinciale - entro due giorni dalla ricezione - eventuali richieste di accesso ex art. 15 del Regolamento 2016/679 UE inoltrate da soggetti terzi;
f) comunicare con immediatezza al Comandante della Polizia Provinciale eventuali accessi non autorizzati da parte di soggetti terzi, negli ambienti in cui risiedono gli schermi e/o le registrazioni;
g) non creare salvataggi dati o banche dati derivanti dalla raccolta effettuata per il tramite dell'impianto di videosorveglianza, senza espressa autorizzazione scritta del Comandante della Polizia Provinciale;
h) mantenere assoluto riserbo sui dati personali di cui vengono a conoscenza nell'esercizio delle loro funzioni;
i) supervisionare i soggetti preposti alla manutenzione dell'impianto quando questi avvengano in loco;
j) prendere visione del presente regolamento, il quale costituisce a tutti gli effetti documento formativo-informativo per un corretto uso della strumentazione necessaria al funzionamento dell'impianto.

I soggetti autorizzati al materiale trattamento devono trattare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle istruzioni del titolare o del responsabile. In ogni caso, prima dell'utilizzo degli impianti, essi saranno istruiti al corretto uso dei sistemi, sulle disposizioni della normativa di riferimento e sul presente regolamento.

Nell'ambito delle persone autorizzate, potranno essere designati, con l'atto di nomina, i soggetti cui è affidata la custodia e conservazione delle chiavi di accesso alla sala di controllo, saranno inoltre rilasciate le credenziali di accesso ai soggetti autorizzati alla visualizzazione, estrapolazione delle immagini e gestione degli applicativi.

3 – Accesso alle basi dati e credenziali

L'accesso alle basi dati è esclusivamente consentito al Responsabile del trattamento e ai soggetti autorizzati come indicato nei punti precedenti. L'accesso alle immagini registrate deve essere effettuato da ciascun operatore esclusivamente nell'ambito del proprio incarico. In nessun caso, i dati trattati, devono essere diffusi o comunicati a terzi, salvo i casi previsti dalla legge. La mancata osservanza degli obblighi previsti comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla legge, responsabilità amministrativa o penale.

I soggetti autorizzati per l'accesso ai sistemi saranno dotati di credenziali univoche (user e password) che devono rispettare i seguenti principi:

a) gli incaricati per effettuare il trattamento delle immagini devono superare apposita procedura di autenticazione;
b) al fine di garantire l'identificazione dell'operatore, si precisa che le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo;
c) con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato;
d) la parola chiave (password) prevista per accedere al sistema di autenticazione è composta da almeno otto caratteri; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni tre mesi;
e) il codice per l'identificazione (user) non sarà assegnato ad altri incaricati, neppure in tempi diversi;
f) le credenziali sono disattivate in caso di perdita della qualifica che consente all'incaricato l'accesso ai dati personali;
g) sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile l'ambiente dove sono visualizzabili le riprese in atto o le relative registrazioni;
h) periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione;
i) l'ingresso alla sala di controllo, ove risiedono i server di archiviazione dei flussi video, è presidiato da sistemi di controllo degli accessi che consentono di abilitare solo il personale incaricato.

4 – Modalità di raccolta e requisiti dei dati personali

I dati personali oggetto di trattamento sono:

a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per le finalità di cui al presente regolamento e resi utilizzabili in altre operazioni del trattamento a condizione che si tratti di operazioni non incompatibili con tali scopi, esatti e, se necessario, aggiornati;
c) raccolti in modo pertinente, completo e non eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati;
d) conservati per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto, per le quali essi sono stati raccolti o successivamente trattati ed in ogni caso pari al periodo di tempo stabilito dalla normativa di riferimento. Nel caso in cui l'Ente voglia procedere a un allungamento dei tempi di conservazione per un periodo superiore si applicano le indicazioni a tale fine fornite dal Garante per la protezione dei dati personali,

configurando in ogni caso tale ipotesi come eccezionale e 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.

I dati personali sono ripresi attraverso le telecamere del sistema di videosorveglianza installate sul territorio provinciale in conformità all'elenco delle aree di ripresa ed in relazione alle esigenze e finalità di cui al presente regolamento. La collocazione delle telecamere può essere modificata, secondo le indicazioni che allo scopo detterà l'Amministrazione Provinciale, mediante appositi atti di indirizzo e gestionali degli Organi competenti.

I dispositivi utilizzati per la raccolta delle immagini dovranno essere conformi alla normativa vigente.

I dati raccolti verranno trasmessi alla sala di controllo utilizzando una linea prevalentemente dedicata allo scopo e idoneamente dimensionata. I dati verranno poi visionati in remoto su dispositivi in uso alla Polizia Provinciale per controlli mirati ed attività d'istituto. Queste postazioni consentono la visualizzazione dei flussi video o la ricerca e l'eventuale estrazione di sequenze video registrate. L'impiego del sistema di videoregistrazione è necessario per ricostruire l'evento per le finalità previste dal presente regolamento.

Le telecamere ambientali mobili (*fototrappole)* implementano il salvataggio delle immagini su SD card o su altro supporto di memorizzazione digitale, preventivamente protetto mediante cifratura crittografica, in modo tale che eventuali sottrazioni della telecamera non permettano a terzi di visionare il contenuto dei supporti di memorizzazione.

Per quanto concerne la modalità relativa alla raccolta dei dati mediante dispositivi elettronici per la rilevazione al Codice della Strada si rinvia a quanto previsto dalla legge e dalle norme del presente regolamento.

5 – Obblighi degli operatori

L'utilizzo del brandeggio e dello zoom da parte degli operatori incaricati al trattamento dovrà essere conforme ai limiti indicati nel presente regolamento e comunque attivato esclusivamente in caso di necessità.

L'utilizzo delle telecamere è consentito solo per il controllo di quanto si svolga nei luoghi pubblici mentre esso non è ammesso nelle proprietà private.

Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo ammesso per la conservazione di cui al precedente paragrafo, solo in caso di effettiva necessità per il conseguimento delle finalità previste dalla legge a seguito di regolare autorizzazione richiesta al Responsabile interno del trattamento.

La mancata osservanza degli obblighi previsti al presente articolo comporterà l'applicazione di sanzioni disciplinari e, nei casi previsti dalla legge, di responsabilità amministrative o penali.

6 – Informazioni rese agli interessati

La Provincia di Brescia in ottemperanza a quanto disposto dal Regolamento 2016/679 UE, si obbliga ad affiggere l'informativa in conformità ai modelli semplificati individuati dal Garante per la Protezione dei Dati Personali ai sensi del provvedimento dell'8 aprile 2010 e s.m.i., nelle località in cui sono posizionate le telecamere, prima del raggio di azione delle stesse, anche nelle loro immediate vicinanze e non necessariamente a contatto con gli impianti.

In relazione alla vastità dell'area oggetto di rilevamento ed alle modalità delle riprese, dovranno essere installati più cartelli. Questi ultimi devono avere un formato ed un posizionamento tale da essere visibile in ogni condizione di illuminazione ambientale e possono 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.
La Provincia di Brescia, nella persona del Responsabile interno del Trattamento, comunicherà alla comunità l'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, l'eventuale incremento dimensionale dell'impianto stesso e l'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, con un anticipo di giorni dieci, mediante pubblicazione sul sito istituzionale dell'Ente. Nella già menzionata comunicazione sono contenute almeno le seguenti informazioni:
a) indicazione del Titolare e del Responsabile del trattamento;
b) finalità del trattamento;
c) modalità di utilizzo e di posizionamento delle telecamere;
d) diritti esercitabili dall'interessato;
e) termini di conservazione delle immagini registrate.

Detta informativa può essere reperita sul sito istituzionale dell'Ente senza spese od oneri aggiuntivi a carico dell'interessato.

7 – Diritti degli interessati

Si applicano i precetti richiamati dagli articoli da 12 a 21 del Regolamento 2016/679 UE.
In relazione al trattamento dei dati personali l'interessato, dietro presentazione di apposita istanza, ha diritto:
a) di ottenere la conferma dell'esistenza di trattamenti di dati che possono riguardarlo;
b) di essere informato sugli estremi identificativi del titolare e del responsabile oltre che sulle finalità e le modalità del trattamento cui sono destinati i dati;
c) di ottenere, a cura del responsabile, senza ritardo e comunque non oltre 15 giorni dalla data di ricezione della richiesta, ovvero di 30 giorni previa comunicazione all'interessato se le operazioni necessarie per un integrale riscontro sono di particolare complessità o se ricorre altro giustificato motivo, la conferma dell'esistenza o meno di dati personali che lo riguardano anche se non ancora registrati e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, delle modalità e delle finalità su cui si basa il trattamento; la richiesta non può essere inoltrata dallo stesso soggetto se non trascorsi almeno novanta giorni dalla precedente istanza, fatta salva l'esistenza di giustificati motivi;
d) di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
e) di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.

Nei casi contemplati dalla legge, può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati e comprensivi dei costi del personale, secondo le modalità previste dalla normativa vigente.

I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
Nell'esercizio dei diritti di cui sopra, l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.
L'istanza deve indicare a quale impianto di videosorveglianza si fa riferimento, il giorno e l'ora in cui il richiedente potrebbe essere stato oggetto di ripresa. Qualora tali indicazioni manchino o siano insufficienti a permettere il reperimento delle immagini, di ciò deve essere data comunicazione al richiedente, così come nell'ipotesi in cui le immagini di possibile interesse non siano state oggetto di conservazione. Il responsabile interno del trattamento è tenuto ad accertare l'effettiva esistenza delle immagini dandone comunicazione al richiedente; nel caso di accertamento positivo fissa il giorno l'ora ed il luogo in cui l'interessato possa visionare le immagini che lo riguardano. Le istanze di cui al presente articolo possono essere trasmesse al titolare o al responsabile anche mediante lettera raccomandata o posta elettronica certificata; le stesse saranno prese in carico dal Responsabile interno del Trattamento il quale dovrà provvedere in merito entro e non oltre quindici giorni.
Nel caso di esito negativo all'istanza di cui ai commi precedenti, l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.
Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al Regolamento 2016/679 UE, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento.
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 Regolamento 2016/679 UE, 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.
In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini riguardanti un fatto obiettivo; viceversa, l'interessato ha diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge.

8 – Sicurezza dei dati

I dati raccolti mediante sistemi di videosorveglianza sono trattati con piena assicurazione delle misure di sicurezza previste dal Regolamento 2016/679 UE e dal citato provvedimento del Garante per la Protezione dei Dati Personali del 08/04/2010 e s.m.i., così da ridurre al minimo 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.
Le misure minime di sicurezza dovranno rispettare le seguenti indicazioni:

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

b) laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
c) per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;
d) nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni potranno accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;
e) qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del Codice Penale.

I server di archiviazione dei flussi video del sistema di videosorveglianza della Provincia di Brescia sono ubicati presso i locali di proprietà provinciale, che risultano protetti da idonei sistemi di sicurezza fisica in aggiunta ai sistemi di sicurezza logica applicati al sistema di videosorveglianza, 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.

La piattaforma software di gestione dei dati (immagini) è anch'essa dotata di una funzionalità di controllo degli accessi mediante la creazione di account, con credenziali di autenticazione, a cui saranno abbinati diversi profili operativi differenziati per livelli di visibilità e trattamento delle immagini. La distribuzione delle credenziali e l'associazione con i diversi profili operativi agli operatori incaricati avvengono secondo le indicazioni del Responsabile interno del trattamento dei dati in base ai compiti attribuiti ad ognuno.

La rete utilizzata per il trasporto dei flussi video dalle telecamere ai sistemi di memorizzazione è una rete ad uso esclusivo, chiusa, non interconnessa con altre reti private o pubbliche. Qualora risulti necessaria la trasmissione dei flussi video su una rete pubblica, essa dovrà avvenire su canali protetti da crittografia o preferibilmente su sistemi VPN di comprovata sicurezza. La trasmissione mediante una rete fibra ottica di telecomunicazioni di immagini riprese da apparati di videosorveglianza viene effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza.

9 – Cessazione del trattamento dei dati

In caso di cessazione, per qualsiasi causa, dei presupposti per i quali era stato effettuato un trattamento mediante l'impianto di videosorveglianza, i dati personali saranno distrutti da tutti i supporti di memorizzazione.

10 – Limiti all'utilizzabilità di dati personali

I dati personali sono utilizzati nei limiti previsti dalla normativa in materia di protezione dei dati personali e dal Provvedimento del Garante in materia di videosorveglianza dell'8 aprile 2010 e successive modificazioni e integrazioni.

Appendice: ***<Provvedimento in materia di videosorveglianza>***
<FAQ Videosorveglianza>
Garante per la protezione dei dati personali

PROVVEDIMENTO IN MATERIA DI VIDEOSORVEGLIANZA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

sommario

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

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

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

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

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

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

Relatore il prof. Francesco Pizzetti

1. PREMESSA

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

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

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

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

1. In www.garanteprivacy.it; doc. web n. 1003482.

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

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

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

2. TRATTAMENTO DEI DATI PERSONALI E VIDEOSORVEGLIANZA: PRINCIPI GENERALI

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

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

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

2) protezione della proprietà;

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

4) acquisizione di prove.

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

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

In tale quadro, pertanto, è necessario che:

a) il trattamento dei dati attraverso sistemi di videosorveglianza sia fondato su uno dei presupposti di liceità che il Codice prevede espressamente per i soggetti pubblici da un lato (svolgimento di funzioni istituzionali: artt. 18-22 del Codice) e, dall'altro, per soggetti privati ed enti pubblici economici (es. adempimento ad un obbligo di legge, provvedimento del Garante di c.d. "bilanciamento di interessi" -v., in proposito, punto 6.2- o consenso

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

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

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

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

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

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

libero ed espresso: artt. 23-27 del Codice). Si tratta di presupposti operanti in settori diversi e che sono pertanto richiamati separatamente nei successivi paragrafi del presente provvedimento relativi, rispettivamente, all'ambito pubblico e a quello privato;

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

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

3. ADEMPIMENTI APPLICABILI A SOGGETTI PUBBLICI E PRIVATI

3.1. Informativa

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

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

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

Il supporto con l'informativa:

- deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

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

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

3.1.1. Informativa e sicurezza

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

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

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

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

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

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

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

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

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

Va infine sottolineato che deve essere obbligatoriamente fornita un'idonea in-

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

3.1.3. Informativa da parte dei soggetti privati che effettuano collegamenti con le forze di polizia

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

Al predetto trattamento si applicano le prescrizioni contenute nel punto 4.6.

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

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

3.2. Prescrizioni specifiche

3.2.1. Verifica preliminare

I trattamenti di dati personali nell'ambito di una attività di videosorveglianza devono essere effettuati rispettando le misure e gli accorgimenti prescritti da questa Autorità come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello del titolare (art. 17 del Codice), quando vi sono rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare.

In tali ipotesi devono ritenersi ricompresi i sistemi di raccolta delle immagini associate a dati biometrici. L'uso generalizzato e incontrollato di tale tipologia di dati può comportare, in considerazione della loro particolare natura, il concreto rischio del verificarsi di un pregiudizio rilevante per l'interessato, per cui si rende necessario prevenire eventuali utilizzi impropri, nonché possibili abusi.

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

Un analogo obbligo sussiste con riferimento a sistemi c.d. intelligenti, che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli. In linea di massima tali sistemi devono considerarsi eccedenti rispetto alla normale attività di videosorveglianza, in quanto possono determinare effetti particolarmente invasivi sulla sfera di autodetermi-

nazione dell'interessato e, conseguentemente, sul suo comportamento. Il relativo utilizzo risulta comunque giustificato solo in casi particolari, tenendo conto delle finalità e del contesto in cui essi sono trattati, da verificare caso per caso sul piano della conformità ai principi di necessità, proporzionalità, finalità e correttezza (artt. 3 e 11 del Codice).

Deve essere sottoposto a verifica preliminare l'utilizzo di sistemi integrati di videosorveglianza nei casi in cui le relative modalità di trattamento non corrispondano a quelle individuate nei punti 4.6 e 5.4 del presente provvedimento.

Ulteriori casi in cui si rende necessario richiedere una verifica preliminare riguardano l'allungamento dei tempi di conservazione dei dati delle immagini registrate oltre il previsto termine massimo di sette giorni derivante da speciali esigenze di ulteriore conservazione, a meno che non derivi da una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria in relazione a un'attività investigativa in corso (v. punto 3.4).

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

3.2.2. Esclusione della verifica preliminare

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

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

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

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

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

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

3.2.3. Notificazione

È regola generale che i trattamenti di dati personali devono essere notificati al Garante solo se rientrano in casi specificamente previsti (art. 37 del Codice). In relazione a quanto stabilito dalla lett. f), del comma 1, dell'art. 37, questa Autorità ha già disposto che non vanno comunque notificati i trattamenti di dati effettuati per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio ancorché relativi a comportamenti illeciti o fraudolenti, quando immagini o suoni raccolti siano conservati temporaneamente[11]. Al di fuori di tali precisazioni, il trattamento, che venga effettuato tramite sistemi di videosor-

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

veglianza e che sia riconducibile a quanto disposto dall'art. 37 del Codice, deve essere preventivamente notificato a questa Autorità.

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

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

3.3.1. Misure di sicurezza

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

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

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

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

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

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

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

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

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

3.3.2. Responsabili e incaricati

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

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

Il mancato rispetto di quanto previsto nelle lettere da a) ad f) del punto 3.3.1 comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-ter, del Codice.

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

3.4. Durata dell'eventuale conservazione

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

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

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

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

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

consegnare una copia specificamente richiesta dall'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso.

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

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

3.5. Diritti degli interessati

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

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

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

4. SETTORI SPECIFICI

4.1. Rapporti di lavoro

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

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

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

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

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

4.2. Ospedali e luoghi di cura

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

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

13. Provv. 9 novembre 2005, doc. web n. 1191411.

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

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

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

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

4.3. Istituti scolastici

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

14. Provv. 4 settembre 2009, doc. web n. 1651744.

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

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

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

4.4. Sicurezza nel trasporto pubblico

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

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

4.4.3. I titolari del trattamento dovranno poi provvedere a fornire la prevista informativa agli utenti del servizio di trasporto urbano. Gli autobus, i tram, i taxi ed i veicoli da noleggio con o senza conducente dotati di telecamere dovranno pertanto portare apposite indicazioni o contrassegni che diano conto con immediatezza della presenza dell'impianto di videosorveglianza, anche

utilizzando a tal fine il fac-simile riportato nell'allegato n. 1 al presente provvedimento, e indicanti, comunque, il titolare del trattamento, nonché la finalità perseguita.

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

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

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

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

4.6. Sistemi integrati di videosorveglianza

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

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

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

pubblici, ovvero alle sole finalità riportate nell'informativa, nel caso dei soggetti privati;

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

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

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

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

2) separazione logica delle immagini registrate dai diversi titolari.
Il mancato rispetto delle misure previste ai punti 1) e 2) comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-ter, del Codice.
Fuori dalle predette ipotesi, in tutti i casi in cui i trattamenti effettuati tramite sistemi integrati di videosorveglianza hanno natura e caratteristiche tali per cui le misure e gli accorgimenti sopra individuati non siano integralmente applicabili, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare, il titolare del trattamento è tenuto a richiedere una verifica preliminare a questa Autorità (v. punto 3.2.1).

5. SOGGETTI PUBBLICI

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

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

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

5.1. Sicurezza urbana

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

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

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

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

5.2. Deposito dei rifiuti

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

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

16. D.m. 5 agosto 2008 cit.

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

si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi.

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

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

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

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

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

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

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

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

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

19. V., ad es., art. 3 d.P.R. 22 giugno 1999, n. 250 recante "Regolamento recante norme per l'autorizzazione alla installazione e all'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato, a norma dell'articolo 7, comma 133-bis, della L. 15 maggio 1997, n. 127".

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

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

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

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

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

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

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

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

Come si è detto, la normativa di settore prevede espressamente, in alcuni casi (es., rilevamento a distanza dei limiti di velocità, dei sorpassi vietati), l'obbligo di rendere nota agli utenti l'installazione degli impianti elettronici di rilevamento automatizzato delle infrazioni. In questi stessi casi è quindi possibile fare a meno di fornire un'ulteriore, distinta informativa rispetto al trattamento

dei dati che riproduca gli elementi che sono già noti agli interessati per effetto degli avvisi di cui alla disciplina di settore in tema di circolazione stradale (art. 13, comma 2, del Codice). L'installazione di questi ultimi appositi avvisi previsti dal Codice della strada permette già agli interessati di percepire vari elementi essenziali in ordine al trattamento dei propri dati personali. Pertanto, gli avvisi che segnalano adeguatamente l'attivazione di dispositivi elettronici di rilevazione automatica delle infrazioni possono essere considerati idonei ad adempiere all'obbligo di fornire l'informativa di cui all'art. 13 del Codice.

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

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

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

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

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

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

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

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

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

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

6. PRIVATI ED ENTI PUBBLICI ECONOMICI

6.1. Trattamento di dati personali per fini esclusivamente personali

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

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

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

6.2.1. Consenso

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

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

6.2.2. Bilanciamento degli interessi

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

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

6.2.2.1. Videosorveglianza (con o senza registrazione delle immagini)

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

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

6.2.2.2. Riprese nelle aree condominiali comuni

Qualora i trattamenti siano effettuati dal condominio (anche per il tramite della relativa amministrazione), si evidenzia che tale specifica ipotesi è stata recentemente oggetto di una segnalazione da parte del Garante al Governo ed al Parlamento[22]; ciò in relazione all'assenza di una puntuale disciplina che permetta di risolvere alcuni problemi applicativi evidenziati nell'esperienza di questi ultimi anni. Non è infatti chiaro se l'installazione di sistemi di videosorveglianza possa essere effettuata in base alla sola volontà dei comproprietari, o se rilevi anche la qualità di conduttori. Non è parimenti chiaro quale sia il numero di voti necessario per la deliberazione condominiale in materia (se occorra cioè l'unanimità ovvero una determinata maggioranza).

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

7. PRESCRIZIONI E SANZIONI

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

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

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

TUTTO CIÒ PREMESSO IL GARANTE:

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

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

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

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

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

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

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

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

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

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

Roma, 8 aprile 2010

ALLEGATO n. 1

Per le modalità di utilizzazione del modello, cfr. punto 3.1.

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

ALLEGATO n. 2

Per le modalità di utilizzazione del modello, cfr. punti 3.1.3 e 4.6, lett. c).

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

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Garante per la protezione dei dati personali
Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771 - fax 06 696773785
www.garanteprivacy.it

Per informazioni presso l'Autorità:
Ufficio per le relazioni con il pubblico
Lunedì - Venerdì ore 10.00 - 13.00
e-mail: urp@garanteprivacy.it

A cura del Servizio relazioni
con i mezzi di informazione

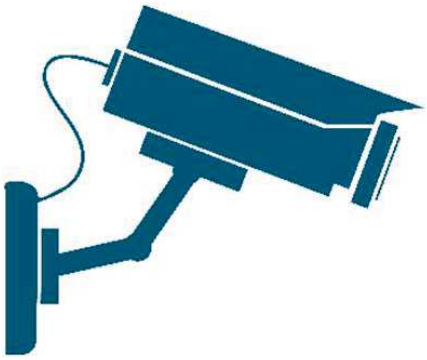
ottobre 2010

Progetto grafico: Vertigo Design

V. 1.0 - Dicembre 2020

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

FAQ



Videosorveglianza

Le risposte alle domande più frequenti (FAQ) in tema di

videosorveglianza e protezione dei dati personali

A CURA DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

1) Quali sono le regole da rispettare per installare sistemi di videosorveglianza?

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: ad esempio, le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, o in materia di controllo a distanza dei lavoratori. Va sottolineato, in particolare, che l'attività di videosorveglianza va effettuata nel rispetto del cosiddetto principio di minimizzazione dei dati riguardo alla scelta delle modalità di ripresa e dislocazione e alla gestione delle varie fasi del trattamento. I dati trattati devono comunque essere pertinenti e non eccedenti rispetto alle finalità perseguite.

E' bene ricordare inoltre che il Comitato europeo per la protezione dei dati (EDPB) ha adottato le *"Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video"* allo scopo di fornire indicazioni sull'applicazione del Regolamento in relazione al trattamento di dati personali attraverso dispositivi video, inclusa la videosorveglianza.

2) Occorre avere una autorizzazione da parte del Garante per installare le telecamere?

No. Non è prevista alcuna autorizzazione da parte del Garante per installare tali sistemi.

In base al principio di responsabilizzazione (art. 5, par. 2, del Regolamento), spetta al titolare del trattamento (un'azienda, una pubblica amministrazione, un professionista, un condominio…) valutare la liceità e la proporzionalità del trattamento, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Il titolare del trattamento deve, altresì, valutare se sussistano i presupposti per effettuare una valutazione d'impatto sulla protezione dei dati prima di iniziare il trattamento (cfr. FAQ n. 7).

3) Le persone che transitano nelle aree videosorvegliate devono essere informate della presenza delle telecamere?

Sì. Gli interessati devono sempre essere informati (ex art. 13 del Regolamento) che stanno per accedere in una zona videosorvegliata, anche in occasione di eventi e spettacoli pubblici (ad esempio, concerti, manifestazioni sportive) e a prescindere dal fatto che chi tratta i dati sia un soggetto pubblico o un soggetto privato.

4) In che modo si fornisce l'informativa agli interessati?

L'informativa può essere fornita utilizzando un modello semplificato (anche un semplice cartello, come quello realizzato dall'EDPB e **disponibile qui**), che deve contenere, tra le altre informazioni, le indicazioni sul titolare del trattamento e sulla finalità perseguita.

Il modello può essere adattato a varie circostanze (presenza di più telecamere, vastità dell'area oggetto di rilevamento o modalità delle riprese).

L'informativa va collocata prima di entrare nella zona sorvegliata.

Non è necessario rivelare la precisa ubicazione della telecamera, purché non vi siano dubbi su quali zone sono soggette a sorveglianza e sia chiarito in modo inequivocabile il contesto della sorveglianza. L'interessato deve poter capire quale zona sia coperta da una telecamera in modo da evitare la sorveglianza o adeguare il proprio comportamento, ove necessario.

L'informativa deve rinviare a un testo completo contenente tutti gli elementi di cui all´art. 13 del Regolamento, indicando come e dove trovarlo (ad es. sul sito Internet del titolare del trattamento o affisso in bacheche o locali dello stesso).

5) Quali sono i tempi dell'eventuale conservazione delle immagini registrate?

Le immagini registrate non possono essere conservate più a lungo di quanto necessario per le finalità per le quali sono acquisite (art. 5, paragrafo 1, lett. c) ed e), del Regolamento). In base al principio di responsabilizzazione (art. 5, paragrafo 2, del Regolamento), spetta al titolare del trattamento individuare i tempi di conservazione delle immagini, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Ciò salvo che specifiche norme di legge non prevedano espressamente determinati tempi di conservazione dei dati (si veda, ad esempio, l'art. 6, co. 8, del D.L. 23/02/2009, n. 11, ai sensi del quale, nell'ambito dell'utilizzo da parte dei Comuni di sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico per la tutela della sicurezza urbana, *"la conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione"*).

In via generale, gli scopi legittimi della videosorveglianza sono spesso la sicurezza e la protezione del patrimonio. Solitamente è possibile individuare eventuali danni entro uno o due giorni. Tenendo conto dei principi di minimizzazione dei dati e limitazione della conservazione, i dati personali dovrebbero essere – nella maggior parte dei casi (ad esempio se la videosorveglianza serve a rilevare atti vandalici) – cancellati dopo pochi giorni, preferibilmente tramite meccanismi automatici. Quanto più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione.

Ad esempio, normalmente il titolare di un piccolo esercizio commerciale si accorgerebbe di eventuali atti vandalici il giorno stesso in cui si verificassero. Un periodo di conservazione di 24 ore è quindi sufficiente. La chiusura nei fine settimana o in periodi festivi più lunghi potrebbe tuttavia giustificare un periodo di conservazione più prolungato.

6) È possibile prolungare i tempi di conservazione delle immagini?

In alcuni casi può essere necessario prolungare i tempi di conservazione delle immagini inizialmente fissati dal titolare o previsti dalla legge: ad esempio, nel caso in cui tale prolungamento si renda necessario a dare seguito ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria in relazione ad un'attività investigativa in corso.

7) Quali sistemi di videosorveglianza necessitano di valutazione d'impatto preventiva?

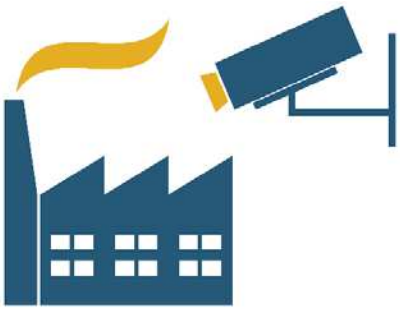
La valutazione d'impatto preventiva è prevista se il trattamento, quando preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per le persone fisiche (artt. 35 e 36 del Regolamento) (per approfondimenti si vedano le **"Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679"** - WP248rev.01 del 4 ottobre 2017).

Può essere il caso, ad esempio, dei sistemi integrati - sia pubblici che privati - che collegano telecamere tra soggetti diversi nonché dei sistemi intelligenti, capaci di analizzare le immagini ed elaborarle, ad esempio al fine di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli.

La valutazione d'impatto sulla protezione dei dati è sempre richiesta, in particolare, in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico (art. 35, par. 3, lett. c) del Regolamento) e negli altri casi indicati dal Garante (cfr. **"Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679"** dell'11 ottobre 2018).

8) Si possono installare telecamere all'interno degli istituti scolastici?

Si rinvia al riguardo alle FAQ sulla scuola disponibili al link **https://www.garanteprivacy.it/home/faq/scuola-e-privacy.**



9) Il datore di lavoro pubblico o privato può installare un sistema di videosorveglianza nelle sedi di lavoro?

Sì, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, nel rispetto delle altre garanzie previste dalla normativa di settore in materia di installazione di impianti audiovisivi e altri strumenti di controllo (art. 4 della l. 300/1970).

10) L'installazione di sistemi di videosorveglianza può essere effettuata da persone fisiche per fini esclusivamente personali, atti a monitorare la proprietà privata?

Sì. Nel caso di videosorveglianza privata, 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, escludendo ogni forma di ripresa, anche senza registrazione di immagini, relativa ad aree comuni (cortili, pianerottoli, scale, parti comuni delle autorimesse) ovvero a zone di pertinenza di soggetti terzi.

È vietato altresì riprendere aree pubbliche o di pubblico passaggio."

11) Quali sono le regole per installare un sistema di videosorveglianza condominiale?

È necessario in primo luogo che l'istallazione avvenga previa assemblea condominiale, con il consenso della maggioranza dei millesimi dei presenti (art. 1136 c.c.).

È indispensabile inoltre che le telecamere siano segnalate con appositi cartelli e che le registrazioni vengano conservate per un periodo limitato. Valgono al riguardo le osservazioni di cui alla FAQ n. 5. In ambito condominiale è comunque congruo ipotizzare un termine di conservazione delle immagini che non oltrepassi i 7 giorni.

12) Si possono utilizzare telecamere di sorveglianza casalinghe c.d. smart cam?

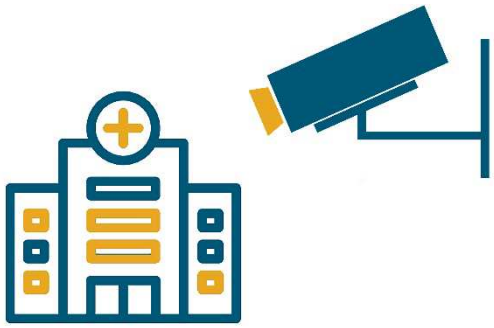
Sì. Il trattamento dei dati personali mediante l'uso di telecamere installate nella propria abitazione per finalità esclusivamente personali di controllo e sicurezza, rientra tra quelli esclusi dall'ambito di applicazione del Regolamento. In questi casi, i dipendenti o collaboratori eventualmente presenti (babysitter, colf, ecc.) devono essere comunque informati dal datore di lavoro.

Sarà comunque necessario evitare il monitoraggio di ambienti che ledano la dignità della persona (come bagni), proteggere adeguatamente i dati acquisiti (o acquisibili) tramite le smart cam con idonee misure di sicurezza, in particolare quando le telecamere sono connesse a Internet, e non diffondere i dati raccolti.

13) I Comuni possono utilizzare telecamere per controllare discariche di sostanze pericolose ed "eco piazzole" per monitorare le modalità del loro uso, la tipologia dei rifiuti scaricati e l'orario di deposito?

Sì, ma solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi e comunque nel rispetto del principio di minimizzazione dei dati. In tal caso, l'informativa agli interessati può essere fornita mediante affissione di cartelli informativi nei punti e nelle aree in cui si svolge la videosorveglianza, che contengano anche indicazioni su come e dove reperire un testo completo contenente tutti gli elementi di cui all´art. 13 del Regolamento (cfr. precedente FAQ n. 4). Non è invece previsto o consentito che tale monitoraggio sia posto in essere da soggetti privati.

14) Si può utilizzare un sistema di videosorveglianza per trattare categorie particolari di dati?



Se le riprese video sono trattate per ricavare categorie particolari di dati, il trattamento è consentito soltanto se risulta applicabile una delle eccezioni di cui all'art. 9 del Regolamento (ad esempio, un ospedale che installa una videocamera per monitorare le condizioni di salute di un paziente effettua un trattamento di categorie particolari di dati personali).

In via generale, ogniqualvolta si installa un sistema di videosorveglianza si dovrebbe prestare particolare attenzione al principio di minimizzazione dei dati. Pertanto, il titolare del trattamento deve in ogni caso sempre cercare di ridurre al minimo il rischio di acquisire filmati che rivelino altri dati a carattere sensibile, indipendentemente dalla finalità.

Il trattamento di categorie particolari di dati richiede una vigilanza rafforzata e continua su taluni obblighi, ad esempio un elevato livello di sicurezza e una valutazione d'impatto sulla protezione dei dati, ove necessario (cfr. FAQ n. 7).

15) I sistemi elettronici di rilevamento delle infrazioni inerenti violazioni del codice della strada vanno segnalate da cartello/informativa?

Sì. I cartelli che segnalano tali sistemi sono obbligatori, anche in base alla disciplina di settore. L'utilizzo di tali sistemi è 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. La ripresa del veicolo non deve comprendere (o deve mascherare), per quanto possibile, la parte del video o della fotografia riguardante soggetti non coinvolti nell'accertamento amministrativo (es. eventuali pedoni o altri utenti della strada). Le fotografie o i video che attestano l'infrazione non devono essere inviati al domicilio dell'intestatario del veicolo, ma l'interessato, ossia la persona eventualmente ritratta nelle immagini, può richiederne copia oppure esercitare il diritto di accesso ai propri dati (fermo restando che dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo).

16) Ci sono casi di videosorveglianza in cui non si applica la normativa in materia di protezione dati?

Sì. La normativa in materia di protezione dati non si applica al trattamento di dati che non consentono di identificare le persone, direttamente o indirettamente, come nel caso delle riprese ad alta quota (effettuate, ad esempio, mediante l'uso di droni). Non si applica, inoltre, nel caso di fotocamere false o spente perché non c'è nessun trattamento di dati personali (fermo restando che, nel contesto lavorativo, trovano comunque applicazione le garanzie previste dall'art. 4 della l. 300/1970) o nei casi di videocamere integrate in un'automobile per fornire assistenza al parcheggio (se la videocamera è costruita o regolata in modo tale da non raccogliere alcuna informazione relativa a una persona fisica, ad esempio targhe o informazioni che potrebbero identificare i passanti).

PER APPROFONDIMENTI E ULTERIORI INFORMAZIONI

www.gpdp.it/temi/videosorveglianza

www.gpdp.it/faq

EDPB - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video (adottate il 29 gennaio 2020) - https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_it

Cartello videosorveglianza - Modello semplificato

urp@gpdp.it