

SESSIONE FORMATIVA ON LINE CORSO DI PERFEZIONAMENTO

GESTIONE DEGLI IMPIANTI DI VIDEOSORVEGLIANZA E DISCIPLINA PER IL CONTROLLO DEL LAVORATORE

Autore Dott.ssa Gloriamaria Paci

Ai sensi dell'art. 5 della legge 22 aprile 1941 n. 633 sulla protezione del diritto d'autore, i testi degli atti ufficiali dello Stato e delle amministrazioni pubbliche, sia italiane che straniere, non sono coperti da diritti d'autore. Il copyright indicato si riferisce all'elaborazione e alla forma di presentazione dei testi stessi. E' contro la legge riprodurre o trasmettere questa pubblicazione in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, incluso fotocopia e registrazione, per scopi diversi dall'esclusivo uso personale dell'acquirente, senza permesso scritto dell'autore



Studio Paci & C. Srl
Studio Consulenza Privacy Dott.ssa Gloriamaria Paci
Via Edelweiss Rodriguez Senior, 13
47924 Rimini (Rn)

Telefono: 0541 – 1795431
Telefax: 0541 - 1794118
Cellulare: 347-5244264
Mail: info@consulenzepaci.it
Sito web: www.consulenzepaci.it

Seguici sui social!
<https://linktr.ee/studiopaci>



Associazione Protezione Diritti e Libertà Privacy APS

Via Edelweiss Rodriguez Senior, 13

47924 Rimini (Rn)

Tel. 0541-1795431 / Fax 0541-1794118

Cell. Gloriamaria Paci 347-5244264

segreteria@associazionedirittiprivacy.it

posta@pec.associazionedirittiprivacy.it

www.associazionedirittiprivacy.it

Seguici sui social!

<https://lintr.ee/apdlp>

Gloriamaria Paci



Nata a Rimini nel gennaio del 1969, dopo alcuni anni dedicati alla carta stampata, nel 1998 Gloriamaria decide di scommettere ed investire in un settore allora poco conosciuto: la normativa sulla tutela dei dati personali.

L'esperienza di giornalista pubblicista, affiancata a quella di consulente privacy nel settore pubblico e privato, sia sul territorio italiano che in paesi Extra UE (RSM), verrà impiegata per pubblicare numerosi articoli e testi di settore.

Relatrice a convegni, seminari e corsi di formazione, con l'introduzione del Regolamento Europeo 2016/679, oggi ricopre il ruolo di Responsabile per la protezione di dati personali per privati ed enti pubblici.

Presidente dell'Associazione protezione diritti e libertà privacy, porta avanti progetti ed iniziative finalizzate all'aggregazione di quanti sono interessati alla salvaguardia dei diritti e delle libertà personali nell'ambito della protezione dei dati.

Luca Di Leo

Consulenza e formazione in materia di protezione dei dati personali dal 2005

Studio Paci & C. Srl
(cda)

Associazione Protezione diritti e libertà privacy APS
(Vice presidente)



Contatti:

dileo@studiopaciecsrl.it

Cell. 3931019939

www.consulenzepaci.it

Linkedin: #luca di leo

Responsabile della Protezione dei Dati (DPO per aziende private, pubbliche, sanità)
certificazione UNI 11697:2017 (Registro Accredia)

Valutatore Privacy
certificazione UNI 11697:2017 (Registro Accredia)

Privacy Officer
Certificazione TUV Italia 2013 – certificazione competenze Federprivacy – Legge n.4/2013

Auditor GDPR
secondo lo schema di certificazione per il GDPR: ISDP@10003 (Registro AICO SICEV)

Consulente per l'implementazione dello schema di certificazione ISDP@10003
(Ente di certificazione INVEO)

Lead Auditor ISO 27001 , aggiornamento ISO 27701

IN LINEA GENERALE

Non tutto ciò che la tecnologia rende possibile è anche giuridicamente lecito

La videosorveglianza non è di per sé indispensabile se esistono altri mezzi per raggiungere lo scopo che si vuole raggiungere. Altrimenti si rischia di modificare le norme culturali con la conseguenza di ammettere come regola l'assenza di privacy

VIDEOSORVEGLIANZA

Normativa privacy

Il trattamento dei dati personali comporta l'applicazione di regole normative unitamente alle indicazioni del Garante

E' necessario ricordare che per l'installazione e l'utilizzo di impianti di videosorveglianza ci sono precetti e regole da osservare, pena l'applicazione di **sanzioni (amministrative e/o penali)**

Il tutto fermo l'obbligo di **risarcire il danno** eventualmente arrecato

Un po di storia

Videosorveglianza

Legge n. 675/96

Il trattamento mediante sistemi di videosorveglianza
esisteva già con la Legge n. 675/96

Telecamere in discoteca.
Multa per mancata informativa ai clienti
Ex. Articolo 10 legge n. 675/96

La qualità delle immagini riprodotte dal sistema di videosorveglianza consentiva la piena riconoscibilità dei clienti in volta
inquadrati

Sanzione nella misura ridotta di 516, 46 euro
da pagarsi entro 60 giorni dalla notifica

Un po di storia
Videosorveglianza
Legge n. 675/96

Videosorveglianza.

**Il Garante fissa in dieci punti le regole
per non violare la privacy**

- 2 Dicembre 2000

PRIVACY E VIDEOSORVEGLIANZA

Provvedimento Generale
Garante protezione dati personali
8 aprile 2010

Chi intende installare impianti per la videosorveglianza deve rispettare
i “principi fondamentali” delineati dal D.Lgs. n 196/03

Il Provvedimento del Garante dell'8 Aprile 2010

1. Mere indicazioni a carattere divulgativo (154.1.h)

2. Prescrizioni impartite con efficacia vincolante (154.1.c)
(Sanzione per l'inosservanza: € 30.000,00 -180.000,00, ex art. 162.2-ter)

I PRINCIPI GENERALI

Principio di liceità

I soggetti pubblici possono effettuare riprese quando siano necessarie allo svolgimento di funzioni istituzionali

I soggetti privati possono effettuare riprese per adempiere ad obblighi di legge o per tutelare un legittimo interesse

I PRINCIPI GENERALI

Principio di necessità

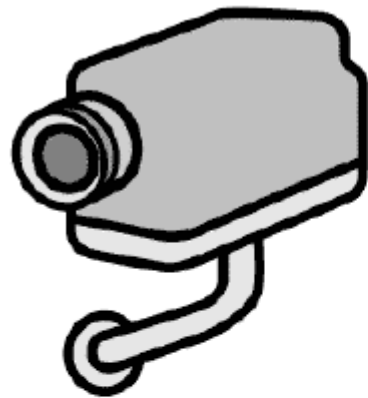
**Analisi sul possibile impiego di strumenti meno
invasivi**

**Verifica se le stesse finalità possono essere
raggiunte con altri strumenti**

**Il sistema informatico va configurato già all'origine in modo da
non utilizzare dati che permettono di identificare le persone
qualora per il raggiungimento delle finalità del trattamento non
sia necessario**

OBBLIGO DI INFORMATIVA SEMPLIFICATA

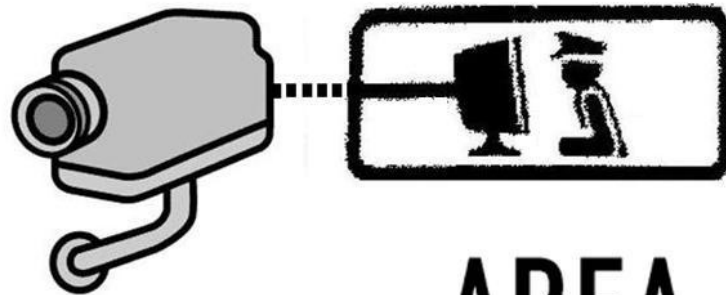
Provvedimento Garante 8 Aprile 2010



**AREA
VIDEOSORVEGLIATA**

La registrazione è effettuata da per fini di

Art. 13 del Codice in materia di protezione dei dati personali (d.lg. n. 196/2003)



**AREA
VIDEOSORVEGLIATA**

La registrazione è effettuata da per fini di

Art. 13 del Codice in materia di protezione dei dati personali (d.lg. n. 196/2003)

ESEMPI DI INFORMATIVE INIDONEE

- 1. Questo esercizio è servito da un sistema di videosorveglianza**
- 2. Attenzione: locali muniti di sistema di videosorveglianza**
- 3. In questi locali sono attive telecamere di controllo**



INFORMATIVA

- 1. Il cartello deve essere affisso nei luoghi ripresi o nelle immediate vicinanze, non necessariamente a contatto con la telecamera**
- 2. Formato e posizionamento visibile anche nelle ore notturne**
- 3. Precisare se è presente rilevazione o registrazione delle immagini**

VERIFICHE PRELIMINARI

Provvedimento Garante Privacy

8 Aprile 2010

In caso di trattamenti che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati

Verifica preliminare in caso di digitalizzazione o indicizzazione delle immagini (cioè che rendono possibile una ricerca automatizzata o nominativa) o in caso di videosorveglianza c.d. dinamico – preventiva che non si limiti a riprendere statisticamente un luogo, ma rilevi percorsi o caratteristiche fisionomiche (es riconoscimento facciale)

LE MISURE DI SICUREZZA

Sono prescritte misure tecniche ed organizzative che consentano al Titolare di verificare l'attività di chi accede alle immagini o controlla il sistema

Trasmissione (via Internet) dei dati ripresi dalle telecamere al server mediante segnale video criptato

Custodia del server in un locale protetto

Doppia chiave autenticazione

**Differenti competenze -
Livelli di visibilità e trattamento differenti**

LE MISURE DI SICUREZZA

Regolamento interno

Nomina del responsabile per la gestione del sistema di videosorveglianza

Nomina degli incaricati al trattamento dati mediante il sistema di videosorveglianza

Informativa specifica per i dipendenti/collaboratori

CONSERVAZIONE DELLE IMMAGINI

**Deve essere commisurata al tempo necessario al
raggiungimento della finalità perseguita
24 ore il termine ordinario**

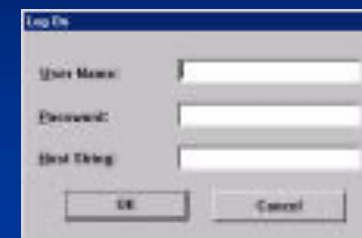
Salvo speciali esigenze (es. festività)

**O specifici casi (es. particolare rischio 7 gg
banche – trasporto valori – aderire ad una specifica richiesta
investigativa dell'autorità giudiziaria o di polizia giudiziaria)**

**Un eventuale allungamento deve essere visto
come eccezionale, e, pertanto, oggetto di verifica preliminare**

I SOGGETTI “IN GIOCO”

Il titolare deve *individuare formalmente* i **soggetti** che hanno accesso alle immagini, i quali vanno **circoscritti** qualitativamente e quantitativamente



NOMINE

Responsabili

Incaricati

Videosorveglianza FAQ del Garante



Videosorveglianza: le FAQ del Garante

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).

Videosorveglianza: le FAQ del Garante

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). Vedi l'immagine del modello semplificato del [cartello videosorveglianza](#).

Videosorveglianza: le FAQ del Garante

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.

Videosorveglianza: le FAQ del Garante

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).

Videosorveglianza: le FAQ del Garante

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."
- Sul tema si raccomanda la consultazione della **scheda informativa** che illustra le principali indicazioni per le persone fisiche che intendono installare, in ambito personale o domestico, sistemi di videosorveglianza a tutela della sicurezza di persone o beni.

Videosorveglianza: le FAQ del Garante

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*)

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

È necessario in primo luogo che l'installazione 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.

Videosorveglianza: le FAQ del Garante

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)

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.
- Sul tema si raccomanda la consultazione della **scheda informativa** che illustra le principali indicazioni per le persone fisiche che intendono installare, in ambito personale o domestico, sistemi di videosorveglianza a tutela della sicurezza di persone o beni.

Videosorveglianza: le FAQ del Garante

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*)

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.

Videosorveglianza: le FAQ del Garante

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)

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).

Videosorveglianza: le FAQ del Garante

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)

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).

Videosorveglianza: le FAQ del Garante

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*)

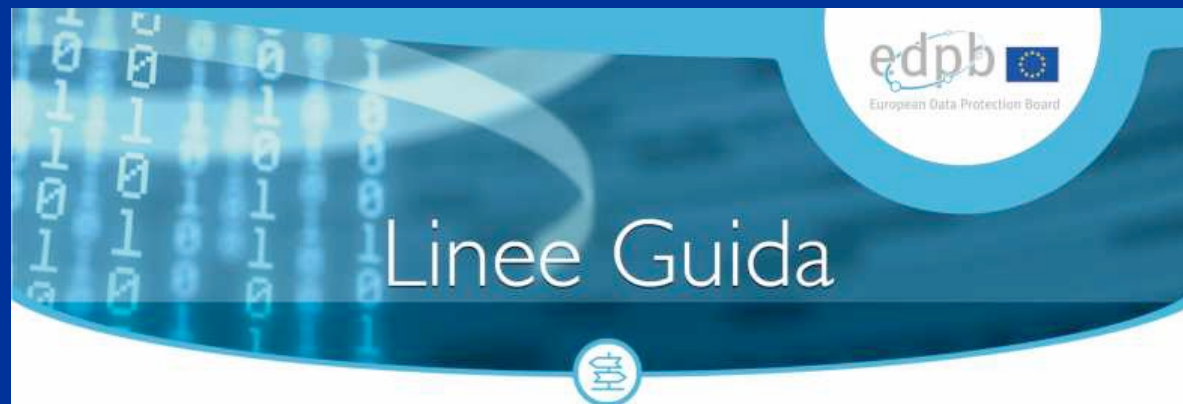
16) Ci sono casi di videosorveglianza in cui non si applica la normativa in materia di protezione dati? Sì. La normativa in materia di protezione dati non si applica al trattamento di dati che non consentono di identificare le persone, direttamente o indirettamente, come nel caso delle riprese ad alta 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).

Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video

Versione 2.0

Adottate il 29 gennaio 2020

Comitato europeo per la protezione dei dati



Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - Versione 2.0 Adottate il 29 gennaio 2020

Le Linee Guida Dell'EDPB prevedono:

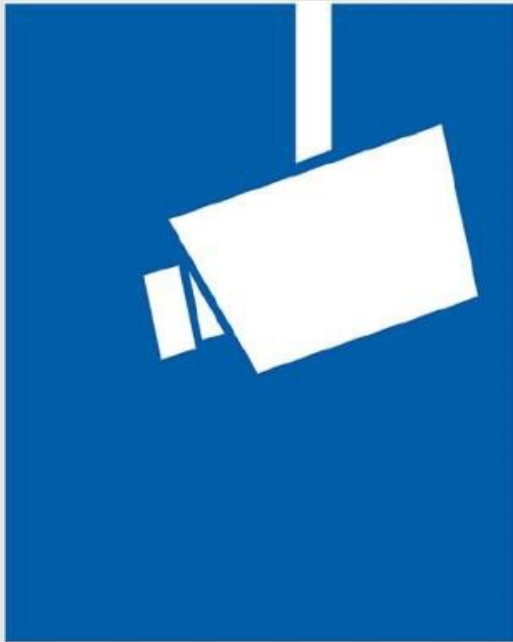
- 1) Adozione di misure tecniche e organizzative**
- 2) La descrizione generale del sistema di videosorveglianza;**
- 3) L'applicazione dei principi di «privacy by design e by default»;**
- 4) La predisposizione della Data Protection Impact Analysis (DPIA) ove necessario.**

I punti più interessanti delle Linee Guida dell'European Data Protection Board

1. **Delimitazione** degli ambiti di applicazione del GDPR, con l'esplicita esclusione dei seguenti casi: telecamere finte, registrazioni effettuate da un'altitudine elevata, videocamere integrate in un autoveicolo per l'assistenza al parcheggio se non raccoglie informazioni relative a una persona fisica e attività puramente personale o domestica
2. Analisi dettagliata del **legittimo interesse** come base giuridica della videosorveglianza: la liceità del trattamento deriva dal un corretto bilanciamento tra gli interessi del **titolare** e quelli degli interessati, dalla necessaria minimizzazione dei dati e dall'impraticabilità di altri sistemi di controllo (meno invasivi) idonei a raggiungere il medesimo scopo
3. **Autonomia normativa** della divulgazione a terzi delle immagini: la comunicazione individuale, la pubblicazione *online* o la messa a disposizione di un filmato a un terzo, comprese le forze dell'ordine, è un processo indipendente, che richiede una giustificazione separata per il soggetto controllore.
4. Necessità di **consenso espresso** e informato per il trattamento di categorie particolari di dati, come i dati biometrici
5. Limiti di **durata** della conservazione dei dati
6. Obbligo di **trasparenza e informazione**: è necessario apporre un cartello di avvertimento con informazioni di primo livello, in combinazione con un'icona per fornire, in modo facilmente visibile, comprensibile e chiaramente leggibile, una visione sommaria del trattamento in concorso con altri strumenti informativi (presidi di secondo livello) da somministrare agli interessati sia in formato digitale sia in formato cartacei. L'avviso va posizionato in un'area che precede la zona monitorata e all'altezza degli occhi degli interessati.

Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video

Comitato europeo per la protezione dei dati



L'informativa completa sul trattamento dei dati è disponibile:

- presso i locali del titolare (reception, casse, ecc.)
- sul sito internet (URL)...
- altro

La registrazione è effettuata da: _____

(inserire i dati di contatto del Responsabile della protezione dei dati personali –DPO, se presente)

Le immagini saranno conservate per un periodo di _____

Finalità della videosorveglianza _____

È possibile accedere ai propri dati ed esercitare gli altri diritti riconosciuti dalla legge rivolgendosi a:

DLgs 151/2015: "Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità", in attuazione della legge 10 dicembre 2014, n. 183"

Titolo II: Disposizioni in materia di rapporto di lavoro e pari opportunità'

Capo I: Disposizioni in materia di rapporto di lavoro

Art. 23 Modifiche all'articolo 4 della legge 20 maggio 1970, n. 300 e all'articolo 171 del decreto legislativo 30 giugno 2003, n. 196

introduce la nuova disciplina in materia di **impianti audiovisivi e altri strumenti di controllo a distanza dei** lavoratori, sostituendo l'articolo 4 della legge n.300/1970 (Statuto dei lavoratori) che a partire dal 1970 disciplinava la materia

La disposizione attua il criterio di delega di cui all'articolo 1, comma 7, lettera f), della legge delega n.183/2014: *"revisione della disciplina dei controlli a distanza, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore"*

Il nuovo art 4 L.300/70 rispetto al previgente testo

Previgente testo dell'Art. 4 L.300/70

“Art. 4. Impianti audiovisivi.

1. È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

2. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi 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.

3. Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.

4. Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale.”

Vigente testo dell'Art 4 L.300/70, ai sensi dell'art 23 [D.Lgs 151/2015](#)

«Art. 4 (Impianti audiovisivi e altri strumenti di controllo). -

1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.».

Le linee-guida si occupano sia dei dispositivi video tradizionali, sia di quelli intelligenti. Per quanto concerne questi ultimi, le Linee-guida si concentrano sulle norme relative al trattamento di categorie particolari di dati. *Altre tematiche affrontate nel documento riguardano, tra l'altro, la liceità del trattamento, l'applicabilità dei criteri di esclusione relativi ai trattamenti in ambito domestico e la divulgazione di filmati a terzi.*

Le linee guida tornano ad occuparsi anche dell'informativa nell'ambito della videosorveglianza. Si tratta di un tema già affrontato dall'Autorità Garante per la Protezione dei dati personali con il noto provvedimento generale prescrittivo in tema di videosorveglianza dell'8 aprile 2010 e recentemente anche dalla Corte di Cassazione, secondo la quale: *"L'installazione di un impianto di videosorveglianza*

all'interno di un esercizio commerciale, costituendo trattamento di dati personali, deve formare oggetto di previa informativa, ex art. 13 del d.lgs. n. 196 del 2003, resa ai soggetti interessati prima che facciano accesso nell'area videosorvegliata, mediante supporto da collocare perciò fuori del raggio d'azione delle telecamere che consentono la raccolta delle immagini delle persone e danno così inizio al trattamento stesso". (Cass. 5 luglio 2016, n. 13663).

Informativa di più livelli

Le linee guida introducono il concetto di informativa a più livelli. In particolare, prevede che: alla luce della quantità di informazioni che devono essere fornite all'interessato, i titolari del trattamento possono seguire un approccio "a più livelli", optando per una combinazione di metodi, al fine di rispettare il principio della trasparenza (WP 260, par. 35; WP 89, p. 22). Con riferimento alla videosorveglianza le informazioni più importanti potrebbero essere mostrate attraverso un cartello (primo livello), mentre le ulteriori informazioni obbligatorie potrebbero essere fornite con altri mezzi (secondo livello)- (Linee guida Capitolo 7, § 109).**84**

Primo e **secondo** **livello**

Proseguono le linee guida specificando come il primo livello riguardi il modo in cui il titolare del trattamento interagisce con l'interessato. In questa fase i titolari possono usare un cartello di avvertimento contenente le informazioni di base. Queste ultime possono essere fornite unitamente ad un'icona al fine di fornire in maniera facilmente visibile, comprensibile e chiaramente leggibile, una panoramica significativa sul trattamento svolto (articolo 12 GDPR, Capitolo 7.1, § 110). È interessante notare come il fac-simile di informativa di primo livello (l'equivalente dell'informativa breve prevista nel Prov. 08.04.2010), oltre a riportare i dati del titolare del trattamento e le finalità del sistema di videosorveglianza, riporta gli estremi del Data protection officer ove presente. Infine, un qr code al quale in maniera semplice l'interessato può accedere all'informativa di secondo livello, più dettagliata.

Distanza

Infine, le linee guida precisano che le informazioni dovrebbero essere posizionate ad una distanza ragionevole rispetto ai luoghi ripresi (WP 89, p.22) di modo che l'interessato possa facilmente essere edotto sulla presenza dell'impianto di sorveglianza prima di farvi ingresso (all'incirca ad una altezza d'uomo). Non è necessario specificare la precisa ubicazione dell'apparecchiatura di sorveglianza, purché non vi siano dubbi sull'area soggetta a ripresa e sul contesto della sorveglianza (WP 89, p.22). L'interessato deve essere in grado di stimare l'area oggetto di ripresa, per poterla eventualmente evitare o acquisire un comportamento idoneo (Capitolo 7.1, § 111).

Principi applicabili al trattamento dei dati personali

art. 5 Reg. UE 2016/679

Trattamento dati: «Videosorveglianza»

- a) trattati in modo lecito, corretto **e trasparente** nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**«minimizzazione dei dati»**);
- d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o **rettificare tempestivamente** i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
- f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Principi applicabili Art. 3 D.Lgs. 51/2018

Trattamento dati: «Videosorveglianza»

- a) trattati in modo **lecito e corretto**;
 - b) raccolti per finalita' determinate, **espresse** e legittime e trattati in modo compatibile con tali finalita';
 - c) **adeguati, pertinenti e non eccedenti** rispetto alle finalita' per le quali sono trattati;
 - d) **esatti e, se necessario, aggiornati**; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalita' per le quali sono trattati;
 - e) conservati con modalita' che consentano l'identificazione degli interessati per il tempo necessario al conseguimento delle finalita' per le quali sono trattati, **sottoposti a esame periodico per verificarne la persistente necessita' di conservazione, cancellati o anonimizzati una volta decorso tale termine**;
 - f) trattati in modo da garantire un'adeguata sicurezza e protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali, mediante l'adozione di misure tecniche e organizzative adeguate.
2. Il trattamento per una delle finalita' di cui all'articolo 1, comma 2, diversa da quella per cui i dati sono raccolti, **e' consentito se il titolare del trattamento, anche se diverso da quello che ha raccolto i dati, e' autorizzato a trattarli per detta finalita'**, conformemente al diritto dell'Unione europea o dell'ordinamento interno e se il trattamento e' necessario e proporzionato a tale diversa finalita', conformemente al diritto dell'Unione europea o dell'ordinamento interno.
3. Il trattamento per le finalita' di cui all'articolo 1, comma 2, puo' comprendere l'archiviazione nel pubblico interesse, l'utilizzo scientifico, storico o statistico, fatte salve le garanzie adeguate per i diritti e le liberta' degli interessati.

Videosorveglianza per fini personali



GPDP

**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Sistemi di VIDEOSORVEGLIANZA installati da PERSONE FISICHE

Le REGOLE da seguire



Le persone fisiche possono, nell'ambito di attività di carattere personale o domestico, attivare sistemi di videosorveglianza a tutela della sicurezza di persone o beni senza alcuna autorizzazione e formalità, purché:



le telecamere siano idonee a riprendere SOLO aree di PROPRIA ESCLUSIVA PERTINENZA;



vengano attivate MISURE TECNICHE PER OSCURARE PORZIONI DI IMMAGINI in tutti i casi in cui, per tutelare adeguatamente la sicurezza propria o dei propri beni, sia inevitabile riprendere parzialmente anche AREE di TERZI;



nei casi in cui sulle aree riprese insista una SERVITÙ DI PASSAGGIO in capo a terzi, sia acquisito formalmente (una tantum) il CONSENSO del soggetto titolare di tale diritto;



NON siano oggetto di ripresa AREE CONDOMINIALI COMUNI o di TERZI;



NON siano oggetto di ripresa AREE APERTE AL PUBBLICO (strade pubbliche o aree di pubblico passaggio);



NON siano oggetto di COMUNICAZIONE A TERZI o di DIFFUSIONE le immagini riprese.

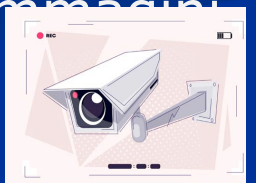
La scheda ha finalità meramente divulgative. Per una piena e corretta comprensione degli adempimenti, si raccomanda la consultazione della normativa in materia e dei provvedimenti del Garante.

Sistemi di VIDEOSORVEGLIANZA installati da PERSONE FISICHE

Le REGOLE da seguire

Le persone fisiche possono, nell'ambito di attività di carattere personale o domestico, attivare sistemi di videosorveglianza a tutela della sicurezza di persone o beni senza alcuna autorizzazione e formalità, purché:

- ✓ Le telecamere siano idonee a riprendere SOLO aree di PROPRIA ESCLUSIVA PERTINENZA;
- ✓ Vengano attivate MISURE TECNICHE PER OSCURARE PORZIONI DI IMMAGINI in tutti i casi in cui, per tutelare adeguatamente la sicurezza propria o dei propri beni, sia inevitabile riprendere parzialmente anche AREE di TERZI;
- ✓ Nei casi in cui sulle aree riprese insista una SERVITÙ DI PASSAGGIO in capo a terzi, sia acquisito formalmente (una tantum) il CONSENSO del soggetto titolare di tale diritto;
- ✓ NON siano oggetto di ripresa AREE CONDOMINIALI COMUNI o di TERZI;
- ✓ NON siano oggetto di ripresa AREE APERTE AL PUBBLICO (strade pubbliche o aree di pubblico passaggio);
- ✓ NON siano oggetto di COMUNICAZIONE A TERZI o di DIFFUSIONE le immagini riprese.



Grazie per l'attenzione

