13 febbraio 2024 - ore 15,00

VIDEOSORVEGLIANZA E FOTOTRAPPOLE CONTRO GLI ABBANDONI E I DEPOSITI INCONTROLLATI DI RIFIUTI

TUTELA DELL'AMBIENTE E TUTELA DELLA PRIVACY A CONFRONTO

Gaetano Alborino

ASMEL Associazione per la Sussidiarietà e la Modernizzazione degli Enti Locali

www.asmel.eu

800165654

webinar@asmel.eu

IL NUOVO TESTO UNICO DELL'AMBIENTE

Il Decreto Legislativo 3 Aprile 2006 n. 152 è vigente dal 29 aprile 2006.

Il T.U. dell'Ambiente è stato recentemente innovato con modifiche importanti, dal D. Lgs. 3 settembre 2020 n. 116/2020, che ha recepito il "Pacchetto economia circolare"; dal D.L. 77/2021 (cd. "Semplificazioni bis"), convertito in Legge 29 luglio 2021, n. 108; poi ancora dalla Legge 17 maggio 2022, n. 60; dal D. Lgs. 23 dicembre 2022, n. 213, vigente dal 16 giugno 2023; infine dal D.L. n. 105/2023, convertito nella Legge 9 ottobre 2023, n. 137

Le norme in materia di gestione dei rifiuti e di bonifica dei siti inquinati sono dettate nella parte quarta del Testo Unico.

L’abbandono e il deposito incontrollato di rifiuti

Articolo 192, commi 1 e 2, T.U.

L’abbandono e il deposito incontrollato di rifiuti sul suolo e nel suolo sono vietati.

È altresì vietata l’immissione di rifiuti di qualsiasi genere, allo stato solido o liquido, nelle acque superficiali e sotterranee

SANZIONI AMMINISTRATIVE PER L'ABBANDONO
E IL DEPOSITO INCONTROLLATO NELLA DISCIPLINA PREVIGENTE

Articoli 192, co. 1 e 2, e 255 co. 1

Fatto salvo quanto disposto dall'articolo 256, comma 2, chiunque abbandona o deposita rifiuti ovvero li immette nelle acque superficiali o sotterranee è punito con la

Sanzione da € 300,00 a € 3.000,00.
PMR € 600.

Se l'abbandono riguarda rifiuti pericolosi, la sanzione amministrativa è aumentata fino al doppio.

SANZIONI PENALI PER L'ABBANDONO
E IL DEPOSITO INCONTROLLATO NELLA DISCIPLINA VIGENTE

Articoli 192, co. 1 e 2, e 255 co. 1

Fatto salvo quanto disposto dall'art. 256, comma 2, chiunque abbandona o deposita rifiuti ovvero li immette nelle acque superficiali o sotterranee è punito con la

Ammenda da mille euro a diecimila euro.

Se l'abbandono riguarda rifiuti pericolosi, la pena è aumentata fino al doppio.

… SANZIONI PENALI

Articolo 256, comma 2

Si applicano ai titolari di imprese ed ai responsabili di enti che abbandonano o depositano in modo incontrollato i rifiuti in violazione del divieto di cui all'articolo 192, commi 1 e 2, le seguenti pene:

a) l'arresto da 3 mesi a 1 anno o l'ammenda da 2600 euro a 26.000 euro se si tratta di **rifiuti non pericolosi**

b) l'arresto da 6 mesi a 2 anni e l'ammenda da 2600 euro a 26.000 euro se si tratta di **rifiuti pericolosi**

Depositi di rifiuti nel Codice della strada

Codice della Strada, articolo 15

Atti vietati

1. Su tutte le strade e loro pertinenze è vietato:

f) *depositare rifiuti o materie di qualsiasi specie, insudiciare e imbrattare comunque la strada e le sue pertinenze;*

f-bis) *insozzare la strada o le sue pertinenze gettando rifiuti o oggetti dai veicoli in sosta o in movimento.*

3. *Chiunque viola uno dei divieti di cui al comma 1, lettere … f), è soggetto alla sanzione amministrativa del pagamento di una somma da € 26 a € 102.*

3-bis. *Chiunque viola il divieto di cui al comma 1, lettera f-bis), è punito con la sanzione amministrativa pecuniaria da euro 216 ad euro 866.*

4. *Dalle violazioni di cui ai commi 2,* ***3 e 3-bis*** *consegue la sanzione amministrativa accessoria dell'obbligo per l'autore della violazione stessa del ripristino dei luoghi a proprie spese, secondo le norme del capo I, sezione II, del titolo VI.*

Riferimenti normativi in materia di privacy

Regolamento dell'Unione Europea 27 aprile 2016, n. 679, più noto con la sigla GDPR – General Data Protection Regulation - pubblicato sulla G.U. Europea il 4 maggio 2016, vigente dal 25 maggio 2018

D. Lgs. 30 giugno 2003, n. 196, recante il "Codice in materia di protezione dei dati personali"

D. Lgs. 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 679/2016"

D.P.R. 15 gennaio 2018, n. 15, recante "L'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia"

D. Lgs. 18 maggio 2018, n. 51, recante ***"Attuazione della direttiva (UE) 2016/680,*** *relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali"*

Le principali novità introdotte dal GDPR

Le principali novità introdotte dal Regolamento Generale sulla Protezione dei dati personali possono essere così sintetizzate:

- viene istituita la figura obbligatoria del **Responsabile della protezione dei dati**, incaricato di assicurare una gestione corretta dei dati personali negli enti. Tale figura può essere individuata tra il personale dipendente in organico, oppure è possibile procedere a un affidamento all'esterno, in base a un contratto di servizi;
- viene introdotto il **Registro delle attività del trattamento,** ove sono descritti i trattamenti effettuati e le procedure di sicurezza adottate dall'ente. Il Registro dovrà contenere specifici dati indicati dal RGPD ;
- viene richiesto agli enti l'obbligo, prima di procedere al trattamento, **di effettuare una valutazione di impatto sulla protezione dei dati.** Tale adempimento è richiesto quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche (si pensi, ad esempio, ai dati ottenuti dalla sorveglianza di zone accessibili al pubblico).

Registri dell'attività di trattamento

Anche nell'ambito videosorveglianza, Il titolare e/o il responsabile deve tenere un registro delle attività di trattamento svolte sotto la propria responsabilità.

In particolare tale registro (art. 30.2 GDPR) , nel caso che venga redatto dal Responsabile del trattamento, contiene le seguenti informazioni:

a) il nome e i dati di contatto del responsabile del trattamento, del titolare del trattamento per conto del quale agisce il responsabile del trattamento e del Responsabile della Protezione dei Dati (DPO – artt. dal 37 al 39 del GDPR);

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Il Responsabile del trattamento nell'ambito della videosorveglianza

Nell'ambito della videosorveglianza è frequente il ricorso al responsabile esterno (es. gestione degli impianti) e si rammenta che il ruolo e i compiti del responsabile esterno sono oggetto di verifica durante le ispezioni del Garante.

Il Responsabile della protezione dati

L'istituzione della nuova figura del Responsabile della protezione dei dati è la principale novità normativa del Regolamento europeo che mira al potenziamento del controllo dell'efficacia e della sicurezza dei sistemi di protezione dei dati personali.

Il Responsabile della protezione dei dati è incaricato, infatti, dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati In tal senso il RPD può indicare al Titolari e/o al Responsabile i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento.

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità;

f) verificare la tenuta dei registri del Titolare e del/dei Responsabili sul trattamento.

Il soggetto pubblico quale titolare del trattamento

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). 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.

Provvedimento in materia di videosorveglianza - 8 aprile 2010 - Paragrafo 5

Il Titolare del trattamento: il Comune o il Sindaco?

Ai sensi dell'art. 28 del codice, il titolare del trattamento è la persona giuridica, non il legale rappresentante o l'amministratore e, come già sottolineato in Cass. n. 13657/2916, detto codice deroga al principio della imputabilità personale della sanzione di cui alla legge n. 689/81, configurando nello specifico regime sanzionatorio ivi dettato, un'autonoma responsabilità della persona giuridica.

Tale responsabilità non può ritenersi oggettiva, ma, analogamente a quanto previsto dal D. Lgs. n. 231/2001 in tema di responsabilità da reato degli enti, va configurata come colpa di organizzazione, da intendersi in senso normativo, come rimprovero derivante dall'inottemperanza da parte dell'ente dell'obbligo di adottare le cautele, organizzative e gestionali, necessarie a prevenre la commissione degli illeciti.

Corte di Cassazione, Sez. Civile II, 3 settembre 2020, n. 18292

Adempimenti applicabili a soggetti pubblici e privati

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata.

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 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).

Provvedimento in materia di videosorveglianza - 8 aprile 2010 - Paragrafo 3.1

Le immagini costituiscono dati personali

«Invero, non appare possibile dubitare del fatto che l'immagine costituisca dato personale rilevante ai sensi dell'art. 4, comma 1, lett. b) del D. Lgs. n. 196/2003, trattandosi di dato immediatamente idoneo ad identificare una persona, a prescindere dalla sua notorietà.

Del resto, già questa Corte (Cassazione n. 14346/2012) ha affermato che «non può dubitarsi, nonostante in dottrina sia stato sollevato qualche dubbio al riguardo, che anche l'immagine di una persona, in sé considerata, quando in qualche modo venga visualizzata o impressa, possa costituire "dato personale" ai sensi dell'art. 4, lett. b), del d.lgs. n. 196 del 2003, noto anche come "codice privacy".

In tal senso, invero, depongono specifiche decisioni del Garante per la protezione di dati personali (21 ottobre 1999; 4 ottobre 2007; 18 giugno 2009, n. 1623306), nonché la decisiva circostanza della previsione, nell'ambito del codice privacy, di una specifica norma (art. 134) in materia di videosorveglianza».

Corte di Cassazione, Sezione II civile, 2 settembre 2015, n. 17440

Il principio di limitazione della conservazione

*I dati sono 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»**).*

Regolamento UE n. 679/2016. Articolo 5, comma 1, lett. e)

Le linee giuda 3/2019 sul trattamento dei dati personali attraverso dispositivi video

Il Capo VII – Sez. III – artt. 68-76 – del Regolamento Europeo è rubricato con il titolo: **Comitato europeo per la protezione dei dati.**

Ai sensi dell'articolo 70, paragrafo 1 sexies, del Regolamento 2016/679/UE, che ha abrogato la direttiva 95/46/CE, **il Comitato europeo per la protezione dei dati** ha adottato, **il 29 gennaio 2020,** le linee guida sul trattamento dei dati attraverso dispositivi video.

Le linee guida hanno lo scopo di fornire indicazioni su come applicare il GDPR, in relazione al trattamento dei dati personali attraverso dispositivi video.

Gli esempi non sono esaustivi: il ragionamento generale può essere applicato a tutti i potenziali settori di utilizzo.

Il campo di applicazione del GDPR

Il monitoraggio sistematico e automatizzato di un determinato spazio con mezzi ottici o audiovisivi è diventato un fenomeno significativo dei nostri giorni. Questa attività comporta la raccolta e la conservazione di informazioni su tutte le persone che entrano nello spazio monitorato, identificabili in base al loro aspetto o ad altri elementi specifici.

L'identità di queste persone può essere stabilita sulla base di questi dati. Consente inoltre l'ulteriore trattamento dei dati personali per quanto riguarda la presenza e il comportamento delle persone in questo spazio.

Il rischio potenziale di un uso improprio di questi dati cresce in relazione alla dimensione dello spazio monitorato e al numero di persone che frequentano lo spazio.

Questo fatto è rispecchiato dal regolamento generale sulla protezione dei dati nell'articolo 35, paragrafo 3, lettera c), **che impone l'esecuzione di una valutazione d'impatto sulla protezione dei dati in caso di monitoraggio sistematico di uno spazio accessibile al pubblico su vasta scala,** nonché nell'articolo 37, paragrafo 1, lettera b), **che impone agli incaricati del trattamento di designare un responsabile della protezione dei dati, se il trattamento per sua natura comporta un monitoraggio regolare e sistematico delle persone interessate.**

Il GDPR non si applica al trattamento dei dati quando:

Il regolamento **(Linee guida 3/2019)** non si applica al trattamento di dati che non hanno alcun riferimento a una persona, ad esempio se una persona non può essere identificata, direttamente o indirettamente.

Esempio n. 1): Il GDPR non è applicabile per le telecamere finte (cioè qualsiasi telecamera che non funziona come una telecamera e quindi non elabora dati personali).

Esempio n. 2: Le registrazioni da un'altitudine elevata rientrano nel campo di applicazione del GDPR solo se, date le circostanze, i dati elaborati possono essere collegati a una persona specifica.

Esempio n. 3): Una videocamera è integrata in un'auto per l'assistenza al parcheggio. Se la telecamera è costruita o regolata in modo tale da non raccogliere informazioni relative a una persona fisica (come le targhe o informazioni che potrebbero identificare i passanti) il GDPR non si applica.

il trattamento dei dati personali da parte delle autorità competenti ai fini della prevenzione, delle indagini, dell'accertamento o del perseguimento di reati o dell'esecuzione di sanzioni penali, compresa la tutela e la prevenzione di minacce alla sicurezza pubblica, rientra nella direttiva EU2016/680.

Ci sono caso di videosorveglianza in cui non si applica la normativa in materia di protezione dei 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).*

Garante privacy – FAQ Videosorveglianza 5 dicembre 2020

L’uso dei droni per il contrasto agli illeciti ambientali

Secondo notizie di stampa, dal prossimo autunno 2021, la Polizia Locale di Roma Capitale sarà dotata di nove droni per il monitoraggio ed il controllo del territorio cittadino (illeciti ambientali, depositi incontrollati di rifiuti, roghi tossici, abusi edilizi …).

Con l’avvio dell’istruttoria avviata a fine agosto, il Garante della Privacy intende verificare l’impatto dell’iniziativa sulla privacy delle persone interessate e il puntuale rispetto della normativa in materia di trattamento dei dati.

Roma Capitale, oltre a fornire le informazioni richieste, dovrà inviare copia della valutazione d’impatto o specificare i motivi per i quali non ha ritenuto di doverla effettuare.

Obblighi di trasparenza e di informazione

È un principio assolutamente acclarato, secondo la legislazione europea sulla protezione dei dati, che le persone interessate devono essere consapevoli del fatto che la videosorveglianza è in funzione.

Essi dovrebbero essere informati in modo dettagliato sui luoghi monitorati.

Nell'ambito del GDPR gli obblighi generali di trasparenza e di informazione sono stabiliti dall'articolo 12 GDPR e seguenti.

I responsabili del trattamento possono seguire un approccio a più livelli, scegliendo di utilizzare una combinazione di metodi per garantire la trasparenza.

Per quanto riguarda la videosorveglianza, **le informazioni più importanti dovrebbero essere visualizzate sul cartello stesso (primo livello), mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello).**

Informazioni di primo livello

Il primo strato riguarda il modo primario in cui il responsabile del trattamento si relaziona per la prima volta con l'interessato. In questa fase, i controllori possono utilizzare un cartello di avvertimento con le relative informazioni. Le informazioni visualizzate possono essere fornite in combinazione con un'icona per dare, in modo facilmente visibile, comprensibile e chiaramente leggibile, una visione d'insieme significativa del trattamento previsto.

Posizionamento del segnale di avvertimento (linee guida 3/2019)

Le informazioni devono essere posizionate in modo tale che l'interessato possa riconoscere facilmente le circostanze della sorveglianza prima di entrare nell'area monitorata (approssimativamente all'altezza degli occhi). Non è necessario rivelare la posizione della telecamera, purché non vi siano dubbi su quali aree siano soggette a monitoraggio e il contesto della sorveglianza sia chiarito in modo inequivocabile.

L'interessato deve essere in grado di stimare quale area viene catturata da una telecamera in modo da poter evitare la sorveglianza o adattare il proprio comportamento, se necessario.

L’informativa secondo il Garante Privacy

È stato evidenziato che il supporto con l’informativa non deve essere necessariamente collocato a stretto contatto con gli impianti, ma nelle sue immediate vicinanze e comunque, prima dell’area interessata dalle riprese (cfr. punto 3.1. del citato provvedimento generale).

In casi come quello descritto, anche quando il sistema di videosorveglianza è impiegato per la prevenzione dei reati ambientali (riconducibile all’ambito applicativo dell’art. 53 del Codice e per ciò stesso quindi esonerato dall’obbligo di informativa), si è ritenuto di raccomandare agli enti pubblici di collocare comunque i cartelli contenenti l’informativa perché rendere palese l’utilizzo dei sistemi di videosorveglianza può, in molti casi, svolgere una ulteriore ed efficace funzione di deterrenza, oltre quelle specificamente perseguite (cfr. punto 3.1.2. del provvedimento generale) (nota 18 gennaio 2017).

Garante Privacy – Relazione annuale attività 2017

I dati contenuti in un cartello

I cartelli dovranno riportare:

- Identità e dati di contatto del titolare e/o responsabile del trattamento;
- Finalità e base giuridica del trattamento;
- Periodo di conservazione delle immagini o criteri per determinare tale periodo;
- Diritto di accesso dell'interessato ai propri dati;
- Altre informazioni, di cui agli artt. 13 e 14 predetti.

Naturalmente, non potendo tutte le informazioni elencate agli artt. 13 e 14 Reg. U.E. 2016/679 essere contenute in un cartello, dovrà essere indicato un modo semplice e diretto affinché gli interessati possano reperire le informazioni prescritte (numero telefonico, sito web, indirizzo dell'ente che ha posizionato la fototrappola, etc.).

Peraltro, sarebbe opportuno che il Comune, per maggior chiarezza ed uniformità di prassi, disciplinasse con un regolamento dettagliato l'intera fase delle procedure di posizionamento degli apparecchi, di accertamento delle fattispecie, di verbalizzazione dell'illecito, di estrapolazione dei dati, di visione dei fotogrammi, di conservazione e altro.

Contenuto di primo livello (linee guida 3/2019)

Le informazioni del primo livello (segnale di avvertimento) dovrebbero in genere trasmettere le informazioni più importanti, ad esempio i dettagli delle finalità del trattamento, l'identità del responsabile del trattamento e l'esistenza dei diritti dell'interessato, insieme alle informazioni sui maggiori impatti del trattamento.

Ciò può includere, ad esempio, i dati di contatto del responsabile della protezione dei dati (se del caso).

Deve anche fare riferimento al secondo livello di informazioni più dettagliato e dove e come trovarle.

Esempio:

Identità del Titolare del trattamento:

Dettagli di contatto del Data Protection Officer (DPO/RPD) ove applicabile:

Finalità del trattamento dati personali nonché fonti normative per l'elaborazione:

Diritti dell'interessato: *Sono i diversi diritti dell'interessato al trattamento nei confronti del Titolare, in particolare il diritto di accesso o cancellazione dei dati personali.*

Per tutti i dettagli su questo servizio di videosorveglianza, inclusi i tuoi diritti, consulta le informazioni complete fornite dal Titolare attraverso le opzioni riportate a sinistra.

Informazioni di secondo livello

Anche le informazioni del secondo livello devono essere messe a disposizione in un luogo facilmente accessibile all'interessato.

Il segnale di avvertimento del primo strato deve fare riferimento in modo chiaro alle informazioni del secondo strato. Inoltre, è meglio se le informazioni del primo livello si riferiscono a una fonte digitale (ad esempio il codice QR o l'indirizzo del sito web) del secondo livello.

Tuttavia, le informazioni dovrebbero essere facilmente disponibili anche in forma non digitale.

Dovrebbe essere possibile accedere alle informazioni del secondo livello senza entrare nell'area censita, soprattutto se le informazioni sono fornite in formato digitale (ciò può essere realizzato ad esempio tramite un link). Un altro mezzo appropriato potrebbe essere un numero di telefono che può essere chiamato. In ogni caso, le informazioni fornite devono contenere tutto ciò che è obbligatorio ai sensi dell'articolo 13 GDPR.

Misure tecniche e organizzative

Come stabilito dall'articolo 32, paragrafo 1, RDPP, il trattamento dei dati personali durante la videosorveglianza non solo deve essere legalmente consentito, ma i responsabili del trattamento e gli incaricati del trattamento devono anche proteggerli adeguatamente. Le misure organizzative e tecniche attuate devono essere proporzionate ai rischi per i diritti e le libertà delle persone fisiche, derivanti da distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso ai dati di videosorveglianza.

Ai sensi degli articoli 24 e 25 del GDPR, i responsabili del trattamento devono attuare misure tecniche e organizzative anche al fine di salvaguardare tutti i principi di protezione dei dati durante il trattamento e stabilire i mezzi per l'esercizio dei diritti degli interessati, come definiti negli articoli 15-22 del GDPR.

I responsabili del trattamento dei dati dovrebbero adottare un quadro interno e politiche che garantiscano tale attuazione sia al momento della determinazione dei mezzi per il trattamento sia al momento del trattamento stesso, compresa l'esecuzione di valutazioni d'impatto sulla protezione dei dati quando necessario.

Occorre avere un'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.

Valutazione d’impatto sulla protezione dei dati

Ai sensi dell'articolo 35, paragrafo 1, GDPR, i titolari del trattamento sono tenuti a effettuare valutazioni d'impatto sulla protezione dei dati (DPIA) quando un tipo di trattamento dei dati può comportare un rischio elevato per i diritti e le libertà delle persone fisiche.

L'articolo 35, paragrafo 3, lettera c), del GDPR stabilisce che i titolari del trattamento sono tenuti a effettuare valutazioni d'impatto sulla protezione dei dati se il trattamento costituisce un monitoraggio sistematico di un'area accessibile al pubblico su vasta scala.

È inoltre importante notare che se i risultati della DPIA indicano che il trattamento comporterebbe un rischio elevato nonostante le misure di sicurezza previste dal responsabile del trattamento, allora sarà necessario consultare l'autorità di controllo competente prima del trattamento. I dettagli sulle consultazioni preliminari si trovano all'articolo 36.

Obbligo di valutazione di impatto sulla protezione dei dati

La valutazione di impatto sulla protezione (art. 35 G.D.P.R.) è un documento di valutazione preventiva dei rischi derivanti dal trattamento dei dati che si intende effettuare.

Viene richiesto agli enti l'obbligo, prima di procedere al trattamento, di effettuare una valutazione di impatto sulla protezione dei dati. Tale adempimento è richiesto quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. (Si pensi, ad esempio, ai dati ottenuti dalla sorveglianza di zone accessibili al pubblico).

Questo documento ha l'obiettivo di analizzare in modo puntuale la struttura del trattamento, quali sono le sue finalità e se vengono trattati solo i dati necessari.

Nella redazione di tale documento il titolare del trattamento viene assistito dal responsabile del trattamento dei dati (chi riceve e visiona le immagini riprese), il quale deve poter fornire ogni informazione necessaria alla corretta valutazione dei rischi per la privacy.

Rilevati eventuali rischi per gli utenti, il titolare del trattamento deve poter individuare concrete misure tecnico-organizzative atte a ridurre, o ad annullare del tutto, tali rischi.

Quando, dal documento, emerge che il trattamento dei dati è causa di un rischio relativamente elevato per gli utenti, c'è l'obbligo di interpello preventivo al Garante della Privacy.

Il Garante interviene solo sulla base delle valutazioni fatte dal titolare del trattamento contenute nel documento, indicando ulteriori misure da adottare per ridurre i rischi, fino ad ammonire il titolare o a vietare il trattamento stesso, quindi a vietare l'utilizzo dell'impianto di videosorveglianza mediante telecamere intelligenti.

Quali sistemi di videosorveglianza necessitano di D.P.I.A.?

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.

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.

Garante privacy – FAQ Videosorveglianza 5 dicembre 2020

Sono escluse le foto trappole dalla D.P.I.A.?

In via generale, il GDPR esclude le attività effettuate per la prevenzione di reati.

Quindi se le foto trappole o in via generale i sistemi di videosorveglianza sono impiegati in indagini penali, non vi è alcun bisogno della valutazione di impatto sulla protezione dei dati.

Viceversa, tutte le informazioni acquisite in violazione degli obblighi di valutazione rappresentano una violazione di legge.

Laddove le fototrappole fossero utilizzate per contrastare le violazioni ambientali punite con sanzione amministrative pecuniarie, il privato potrebbe trasmettere un reclamo al Garante Privacy, per l'irrogazione delle relative sanzioni.

Videosorveglianza e depositi di rifiuti

L'utilizzo di sistemi di videosorveglianza per accertare l'uso di discariche abusive o monitorare il deposito dei rifiuti **è lecito solo se non risulta possibile, o si riveli non efficace, il ricorso a sistemi di controllo alternativi.**

L'indicazione è contenuta nella relazione annuale del Garante della privacy (dati 2014), presentata a Roma il 23 giugno 2015, che sempre con riferimento ai rifiuti, segnala il ritorno di grande attualità della tematica relativa al trattamento dei dati personali nell'ambito delle modalità di controllo delle procedure di raccolta differenziata.

Videosorveglianza e depositi di rifiuti

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

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

Provvedimento in materia di videosorveglianza - 8 aprile 2010 - Paragrafo 5.2

I Comuni possono utilizzare telecamere per controllare depositi incontrollati di rifiuti ed eco piazzole per monitorare le modalità del loro uso, la tipologia dei rifiuti sversati 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.

Non è invece previsto o consentito che tale monitoraggio sia posto in essere da soggetti privati.

Garante privacy – FAQ Videosorveglianza 5 dicembre 2020

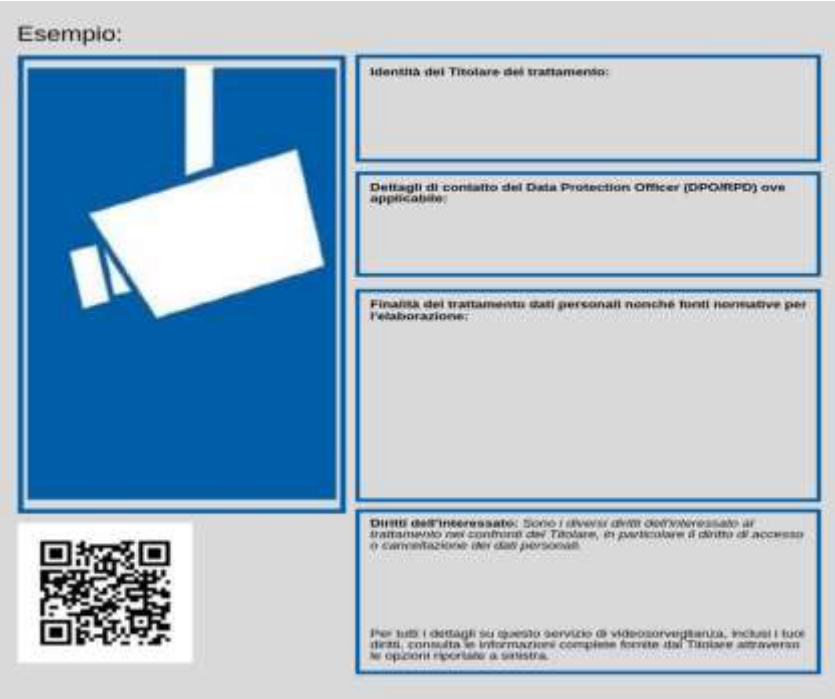
Tutela della privacy nell'uso delle foto trappole

Le foto trappole sono apparecchi che scattano foto o girano video, che possono essere trasmessi a distanza, grazie ad una rete GSM o un wi fi. Il dispositivo si attiva, grazie ad un sensore, al passaggio di un corpo. In origine, tale strumento veniva utilizzato per riprendere la fauna selvatica, senza essere invasiva nei suoi confronti, a fini di interesse scientifico, per riviste o documentari.

Nel tempo, tali dispositivi si sono rivelati utili alle forze di polizia per controllare ampie zone, spesso periferiche o semi-disabitate, anche in assenza o scarsità di personale a disposizione.

La contestuale trasmissione a distanza delle immagini e delle riprese, peraltro, consente di intervenire tempestivamente per accertare e contestare le infrazioni. In particolare, in materia di abbandono dei rifiuti.

Quali adempimenti per l'uso delle foto trappole?



Anche l'uso delle foto trappole pone l'esigenza, al pari di altri sistemi di trattamento dei dati, di tutelare la privacy e proteggere i dati raccolti. L'attivazione del dispositivo, se finalizzata ad attività di polizia amministrativa, **comporta, innanzi tutto, gli obblighi d'informativa con cartelli posti prima del raggio d'azione della telecamera, secondo le prescrizioni degli artt. 13 e 14 del Reg. U.E. 2016/679.**

Anche per finalità di sicurezza e protezione dei beni, nonché prevenzione di furti, se l'area è pubblica o accessibile al pubblico, i cartelli informativi sono necessari; se l'area è privata è sufficiente solo l'autorizzazione del proprietario.

L’orientamento della Procura di Santa Maria C.V.

Ulteriore attività di prevenzione e di contrasto del fenomeno dell'abbandono incontrollato dei rifiuti può essere quella dell'utilizzo dei sistemi di video controllo (ai fini dell'accertamento degli illeciti ambientali), peraltro già adottata da parte di qualche Ente comunale.

Si tratta di apparati mobili c.d. "foto trappole", senza l'utilizzo di cartelli informativi, il cui controllo può essere remotizzato a distanza presso l’Ufficio della Polizia Locale o Provinciale.

Tale utilizzo rientra nell'esercizio delle attività demandate alla polizia giudiziaria ai sensi dell’art. 55 c.p.p.

I singoli Comuni e l’ente Provincia valuteranno, per quanto di propria competenza, la possibilità di installare nell’ambito del proprio territorio comunale e in specie nei luoghi di maggiore allarme detti dispositivi di controllo.

Le Polizie Locali e Provinciali presso le quali possono essere remotizzate le visualizzazioni delle risultanze delle immagini riprese da tali apparecchiature provvederanno agli opportuni monitoraggi e relazioneranno a questa Procura della Repubblica.

Nota Procura della Repubblica di Santa Maria Capua Vetere, 13 aprile 2018, prot. n. 6007

L’orientamento della Procura di Napoli nord

Ulteriore attività di prevenzione e di contrasto del fenomeno dell'abbandono incontrollato dei rifiuti può essere quella dell'utilizzo dei sistemi di video controllo (ai fini dell'accertamento degli illeciti ambientali), peraltro già adottata da parte di svariati Enti comunali.

Si tratta di apparati mobili c.d. "foto trappole", senza l'utilizzo di cartelli informativi, il cui controllo può essere remotizzato a distanza presso l’Ufficio della Polizia Locale o Provinciale.

Il controllo del territorio potrà avvenire anche mediante la sua visualizzazione dall’alto a mezzo di droni.

L‘utilizzo di siffatti strumenti rientra nell'esercizio delle attività demandate alla polizia giudiziaria ai sensi dell‘art. 55 c.p.p.

I singoli Comuni e l’ente Provincia valuteranno, per quanto di propria competenza, la possibilità di installare nell’ambito del proprio territorio comunale e in specie nei luoghi di maggiore allarme detti dispositivi di videocontrollo.

Le Polizie Locali e Provinciali presso le quali possono essere remotizzate le visualizzazioni delle risultanze delle immagini riprese da tali apparecchiature, provvederanno agli opportuni monitoraggi e comunicheranno a questa Procura gli eventuali fatti penalmente rilevanti in tal modo emersi.

Nota Procura della Repubblica di Napoli nord, 27 luglio 2022, prot. n. 682

Sanzioni alla luce del GDPR 679/2016

Art. 83, comma 4

La violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 EUR, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) Gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43.

Art. 83, comma 5

La violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

b) i diritti degli interessati a norma degli articoli da 12 a 22;

L’accertamento del reato in violazione della privacy

«Secondo i condivisibili approdi di questa Corte, ***è legittimamente acquisito ed utilizzato****,* ***ai fini dell’affermazione della responsabilità penale, un filmato effettuato con un telefonino ovvero eseguito grazie ad un sistema di videosorveglianza****, a prescindere dalla conformità alla disciplina sulla privacy, la quale non costituisce sbarramento all’esercizio dell’azione penale* ***(Corte di Cassazione, Sez. V, 28 novembre 2014, n. 2304; Sez. II, 31 gennaio 2013, n. 6812)****».*

Corte di Cassazione, Sez. V, 2 agosto 2021, n. 30191