Videosorveglianza

Prima dell'entrata in vigore del Regolamento Europeo 679/2016 (GDPR) sulla protezione dei dati, che ha apportato numerose e importanti novità alla disciplina "privacy", in tema di videosorveglianza non poteva non tenersi in considerazione il provvedimento del Garante italiano del 10 aprile 2010, che aveva affrontato in materia molto dettagliata il tema.

Con il GDPR e, soprattutto, dopo che il Gruppo dei Garanti Europei, l'EDPB, all'inizio del 2019, aveva già preso posizione su diverse e anche in parte nuove tematiche affacciatesi con l'erompere di molte nuove tecnologie, era atteso un provvedimento nazionale.

Le **Faq dell'Autorità, disponibili da dicembre 2020 sul sito istituzionale** rispondono, in parte, alle attese e contengono indicazioni di cui è opportuno tenere conto[1].

Le questioni affrontate dalle FAQ del Garante privacy

Le regole da rispettare

L'installazione degli impianti deve, innanzitutto, avvenire nel rispetto non solo delle norme in materia di tutela e **protezione dei dati personali** ma anche delle **disposizioni di volta in volta applicabili** (si pensi alla normativa in materia di lavoro e di eventuale controllo dell'attività dei lavoratori, alle norme di carattere penale che sanzionano le illecite interferenze nella vita privata altrui, ecc.).

L'accento dell'Autorità viene posto soprattutto sul c.d. principio di **minimizzazione**, previsto dall'art. 5 del GDPR, che prescrive, in generale, che siano trattati **solo i dati effettivamente necessari, pertinenti e proporzionati rispetto alle finalità** perseguite.

[1] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9496574

Ciò, ovviamente, deve essere riferito anche alle specifiche modalità adottate (si pensi alla possibilità di sola visione delle immagini o anche di registrazione delle stesse, ma anche al posizionamento delle videocamere) e alle funzionalità consentite dall'apparecchio o dal sistema utilizzato (possibilità di rotazione delle camere, zoom, ecc.).

Non serve l'autorizzazione del Garante

In generale non è necessaria un'autorizzazione del Garante: il Regolamento Europeo pone sul soggetto che decida di effettuare un trattamento di dati personali (come deve essere considerata l'operazione di installazione e utilizzo dei sistemi in discorso) l'onere di conoscere e applicare la normativa in materia di privacy, che richiede anche la "giustificazione", motivazione e documentazione delle scelte effettuate (il c.d. principio di **accountability**): di conseguenza la valutazione della liceità o meno dell'installazione dell'impianto (o dell'utilizzo della specifica applicazione) spettano al titolare, sia egli un privato o un'azienda, un gruppo imprenditoriale o un'autorità pubblica.

Le informazioni da fornire: l'informativa "cartello"

E' sempre necessario **informare preventivamente** i soggetti che potrebbero entrare nel raggio di azione delle telecamere.

Questa informazione può essere resa inizialmente con il noto cartello (che è stato "aggiornato" con una nuova versione) ma anche con ulteriori e più dettagliate indicazioni.

Il "cartello" costituisce la c.d. **informativa "breve"** e contiene alcune indicazioni indispensabili (v. il modello qui sotto, proposto dal Gruppo dei Garanti Europei con il provvedimento 3/2019 già citato):

Esso deve innanzitutto:

- essere posto **prima dell'area interessata** dall'azione del sistema, per dare modo alle persone di esserne a preventiva conoscenza e di comprendere quali siano le aree osservate; se l'area di ripresa è estesa, è opportuno che i cartelli siano posizionati in più punti;
- deve **contenere** almeno **l'indicazione del Titolare** del trattamento, ossia del soggetto, dell'ente, dell'autorità che ha deciso di installare l'impianto;
- deve contenere l'indicazione **di quali siano le "finalità"** perseguite dal soggetto che ha deciso di installare l'impianto e, circostanza spesso dimenticata;
- **fare riferimento**, anche eventualmente con modalità tecnologicamente avanzate (QR code, link a siti web) **ad una informativa completa** ai sensi dell'art. 13 del GDPR. Di conseguenza la "sola" apposizione del cartello non esaurisce le prescrizioni in tema di necessarie informazioni agli interessati.

I tempi di conservazione

Il periodo di conservazione, salve specifiche norme di legge, **deve essere deciso dal Titolare** del trattamento, beninteso nel rispetto del principio di responsabilizzazione e di quello di minimizzazione, con la conseguenza che **le immagini registrate non possono essere conservate più a lungo di quanto necessario per le finalità** per le quali sono acquisite.

Il Garante sottolinea come nella gran parte dei casi le videocamere e i sistemi di sorveglianza siano installati per esigenze di sicurezza e di tutela del patrimonio e come molto spesso eventuali danni o eventi lesivi possano essere individuati nell'arco di uno o due giorni. Un periodo di **24 ore appare dunque nella maggioranza dei casi più che adeguato**, salve eventuali protrazioni per ragioni come la chiusura del fine settimana, periodi festivi o altre specifiche necessità.

In ogni caso, quanto più prolungato è il periodo di conservazione (soprattutto se superiore a 72 ore), tanto più argomentate dovranno essere l'analisi e la documentazione relative alla legittimità dello scopo e alla necessità della conservazione.

In alcuni casi può essere necessario prolungare i tempi di conservazione delle immagini inizialmente fissati dal titolare o previsti dalla legge, come avviene allorché il prolungamento si renda necessario per dare seguito ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria in relazione ad un'attività investigativa in corso.

La c.d. "DPIA": la valutazione d'impatto

La valutazione d'impatto è una **particolare procedura** che il Regolamento europeo prevede (si veda l'art. 35) in tutti i casi in cui il trattamento dei dati personali possa presentare un **"rischio elevato" per gli interessati**.

Essa è prevista in particolare se il trattamento prevede l'uso di nuove tecnologie, oppure allorché gli interessati siano soggetti considerati in posizione più "debole" rispetto a chi esegue il trattamento, come avviene nei contesti lavorativi, oppure quando il trattamento riguardi dati di carattere particolare, come oggi sono definiti i dati cc.dd. "sensibili", oppure dati giudiziari, o ancora dati biometrici o genetici.

In realtà e per precisione le ipotesi in cui la DPIA è obbligatoria sono diverse ma, di fatto, in tutte le occasioni in cui un determinato trattamento possa avvenire mediante **strumenti tecnologicamente avanzati o comportare il trattamento di dati considerati più "delicati"**, essa deve essere effettuata (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; il nostro Garante ha pubblicato un elenco di trattamenti che devono essere sottoposti a tale valutazione nell'autunno del 2018).

A scuola e sul luogo di lavoro

Per la scuola il Garante richiama le proprie indicazioni di settore, mentre per quanto riguarda i sistemi installati dal datore di lavoro è imprescindibile ricordare le prescrizioni dell'art. 4 dello Statuto dei lavoratori che, in sintesi, consentono l'installazione esclusivamente in presenza delle finalità costituite da esigenze organizzative e produttive, tutela del patrimonio aziendale, salute e sicurezza sul luogo di lavoro e stabiliscono una precisa procedura per potervi procedere (accordo sindacale o, in mancanza, autorizzazione dell'Ispettorato del Lavoro).

Proprietà privata, smart cam e videosorveglianza

E' sempre possibile l'installazione di sistemi di videosorveglianza da parte di persone fisiche che vogliano **tutelare i propri beni** ma, 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 riprendere aree pubbliche o di pubblico passaggio.

Ciò vale anche per le cc.dd. **smart cam**, installate nelle abitazioni per finalità esclusivamente personali di controllo e di sicurezza, con l'avvertenza che eventuali soggetti "esterni" come collaboratori domestici, baby sitter o dipendenti dovranno essere debitamente e previamente informati dal proprietario di casa (e ricordando che, seppure lo Statuto dei lavoratori non si applichi al lavoro domestico, non sono infrequenti contestazioni su asseriti illeciti utilizzi dei sistemi di cui parliamo).

In tal caso pare comunque opportuno sottolineare un'attenta predisposizione del sistema, sia per quanto riguarda il periodo di conservazione sia soprattutto per quanto riguarda le aree oggetto di visione (evitare i servizi, ad esempio) nonché

le misure di sicurezza da adottare, a maggior ragione se il sistema sia connesso a Internet, come avviene ormai sempre più a motivo della diffusione di sistemi cc.dd. IoT.

Videosorveglianza in condominio

L'installazione da parte del Condominio è **legittima, purché essa avvenga previa delibera condominiale con il consenso della maggioranza dei millesimi dei presenti**, ai sensi dell'art. 1136 codice civile.

Il Garante precisa, richiamando quanto già visto sopra in relazione ai tempi di conservazione, soggetti alla responsabilizzazione del titolare, che sia possibile o, meglio **"congruo"**, in condominio, "ipotizzare **un termine di conservazione delle immagini che non oltrepassi i 7 giorni.**"

Dati di carattere particolare

In generale l'utilizzo di un sistema di videosorveglianza non comporta, di per sé, un trattamento di dati di carattere particolare (dati "sensibili", dati sanitari, ecc.).

Tuttavia allorché il sistema sia utilizzato per ricavare dati di natura particolare, in tal caso il trattamento diviene soggetto a più stringenti limiti e, in particolare, alla necessità che ciò avvenga in presenza di una delle possibili eccezioni previste dall'art. 9 del GDPR.

Ciò accade, ad esempio, non solo nel caso di un ospedale che installi sistemi di videosorveglianza per monitorare lo stato di salute dei pazienti, ma anche allorché ad esempio un sistema video catturi il viso di un soggetto e ne esegua un trattamento al fine, ad esempio, di riconoscerlo.

Tale complessa tipologia di trattamenti comporta una ben più consistente necessità di cautele e di rispetto di normative, che ci sentiamo di suggerire di osservare con scrupolo.

Eco – piazzole, infrazioni stradali

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. Ciò peraltro solo se non risulti 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.

Previa idonea cartellonistica possono essere utilizzati sistemi elettronici di rilevamento delle violazioni del codice della strada.

I cartelli che segnalano tali sistemi sono obbligatori, anche in base alla disciplina di settore.

La ripresa del veicolo non deve comprendere la parte del video o della fotografia riguardante soggetti non coinvolti nell'accertamento.

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.

Le esclusioni

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 quanto previsto dallo Statuto dei Lavoratori) 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).

Vale la pena, tuttavia, ricordare che, pur non costituendo trattamento di dati personali, alcune decisioni dell'Autorità Giudiziaria, in relazione alle telecamere finte o non funzionanti, ne hanno evidenziato i profili di possibile responsabilità derivanti dal c.d. principio dell'apparenza del diritto (Cass.,Sez.IIIciv.,n.2311/1995).

Videosorveglianza e adempimenti in base al G.D.P.R.

Premesse le "novità" in tema di videosorveglianza, il complessivo trattamento di dati personali effettuato con tale modalità deve essere complessivamente eseguito secondo i principi generali stabiliti dal Regolamento Europeo n. 679/2016 (il GDPR).

Senza pretesa di completezza e con l'avvertimento che ogni situazione dovrà essere verificata con particolare riguardo al contesto e all'ambito in cui viene predisposta e con la dovuta attenzione ad eventuali profili di rischio che le particolari condizioni di installazione potrebbero suggerire, indichiamo qui di seguito le questioni fondamentali da affrontare.

Principi generali

L'attività di videosorveglianza può generalmente essere effettuata per finalità di:

- protezione ed incolumità degli individui;
- sicurezza e tutela del patrimonio.

E' fondamentale avere presente, però, che l'installazione e l'utilizzo di un impianto di videosorveglianza non deve determinare un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali delle persone riprese.

Di conseguenza è necessario rammentare e osservare le norme in materia di

- **protezione dei dati personali** ma anche quelle dello
- **Statuto dei lavoratori** in relazione alle problematiche connesse al possibile controllo a distanza dell'attività lavorativa dei dipendenti nonché, in generale,
- le norme dell'ordinamento penale.

Il trattamento deve sempre essere effettuato nell'osservanza dei principi fondamentali in materia di protezione dei dati e, di conseguenza di quanto stabilito dall'art. 5 del GDPR, che stabilisce che i dati personali sono:

1. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**»);
2. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità … («**limitazione della finalità**»);
3. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);
4. 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**»);
5. 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 (… «**limitazione della conservazione**»);
6. 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**»).

Il Titolare del trattamento è il soggetto (o l'ente) deputato all'osservanza di tali principi e deve essere in grado di dimostrare di averlo fatto (accountability).

Il registro delle attività di trattamento

Un primo importante adempimento è quello di indicare adeguatamente la videosorveglianza nel "**registro delle attività del trattamento**" di cui all'art. 30 del GDPR e ciò

- sia che si tratti di attività svolta dal Titolare (lo Studio professionale per la protezione del proprio patrimonio)
- sia che, invece, il sistema sia stato installato a seguito di delibera assembleare condominiale: ne deriva che in tal caso la videosorveglianza, di "titolarità" dell'Ente, è opportuno che sia inserita tra le indicazioni delle

attività svolte dall'amministratore o dallo studio insieme alle altre demandate dall'Ente in virtù del rapporto in essere.

L'Informativa

Come già precisato, gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata, mediante apposizione del "nuovo" cartello,

- prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
- 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, come anche un QR Code che rimandi ad una Informativa completa;
- se sono posizionate più telecamere, dovranno essere esposti più cartelli.

Qualora venga richiesto, il Titolare è tenuto a fornire, anche tramite un apposito soggetto debitamente incaricato, un'informativa adeguata (anche oralmente) contenente tutti gli elementi necessari.

I soggetti autorizzati al trattamento (dipendenti e collaboratori dello Studio dell'Amministratore oppure uno o più Condòmini debitamente incaricati).

Il Titolare (che nel caso dell'Ente Condominiale è ritenuto essere l'Ente stesso) o il Responsabile del trattamento (che, come noto, è la "funzione" che il Garante della Privacy assegna usualmente all'Amministratore di Condominio), devono individuare, **autorizzare e istruire per iscritto** le persone fisiche che possano accedere alle immagini, si tratti di:

- **collaboratori o dipendenti di studio** oppure di
- **portiere, custode** o di altre persone (come ad es. specifici Condòmini cui sia affidata tale mansione).

In corrispondenza alle singole mansioni attribuite ad ogni singolo incaricato/operatore il Titolare e/o il Responsabile del trattamento deve individuare gli ambiti di accesso consentiti (es.: registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).

Nelle nomine dovranno essere specificate anche le singole mansioni attribuite ad ogni operatore, quale l'accesso ai locali ove sono situate le postazioni di controllo, l'utilizzo degli impianti, la visione delle immagini e l'esecuzione di altre attività (quali ad es: registrazione, copiatura, cancellazione, ecc.).

L'individuazione delle società fornitrici del servizio, i Responsabili del trattamento

Il GDPR impone che ogni qualvolta un determinato trattamento sia "esternalizzato", ossia demandato a enti, organizzazioni, società o professionisti terzi (che non rivestano, a loro volta, la qualifica di Titolari del trattamento), tale trattamento debba essere disciplinato da **un contratto** o da altro atto giuridico che vincoli il Responsabile e in cui siano stipulati la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, tenendo conto dei compiti e responsabilità specifici del responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato.

Ancora, l'art. 28 del Regolamento dispone che il Titolare ricorra unicamente a Responsabili che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative e che soddisfino i requisiti della normativa cogente in materia di protezione dei dati, ivi compreso il profilo relativo alla sicurezza, e garantiscano la tutela dei diritti degli interessati.

A tal fine è quindi necessario contrattualizzare il rapporto con la Società che fornisca il servizio o controllare attentamente le Condizioni Generali di contratto o di servizio della specifica **applicazione web o app mobile** mediante la quale si intenda procedere alla gestione del sistema: in tale contratto devono essere attentamente indicati compiti, limiti, attribuzioni e obblighi del responsabile.

Le 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, 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.

Il Titolare deve adottare specifiche misure tecniche ed organizzative che consentano di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa.

Le misure, che possono variare in relazione ai soggetti, alle finalità perseguite nonché in relazione ai sistemi tecnologici utilizzati, devono comunque essere **rispettose dei principi generali** che abbiamo già indicato ma che sono estremamente importanti in ogni tipologia di trattamento (previsione di diversi livelli di visibilità e trattamento delle immagini a seconda delle competenze attribuite ai singoli operatori; attribuzione di credenziali di autenticazione; limitazione, in presenza di sistemi configurati per la registrazione e successiva conservazione delle immagini rilevate, della 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; previsione di misure tecniche od organizzative che consentano di effettuare, allo scadere del termine previsto (massimo 7 giorni, come abbiamo visto), la cancellazione delle immagini (spesso eseguita mediante sovrascrittura delle stesse con un nuovo ciclo di registrazione).

E' opportuno ricordare che in caso di **interventi di manutenzione** sugli impianti di videosorveglianza i soggetti preposti alle operazioni possono accedere alle immagini solo se ciò sia indispensabile e solo in presenza dei soggetti debitamente autorizzati.

Coiem già segnalato, è doveroso che laddove si utilizzino sistemi di videosorveglianza gestiti mediante applicativi web o app mobile siano implementate ulteriori e adeguate misure di protezione (credenziali e password robuste, cifratura, limitazioni di accesso, ecc.).

Diritti degli interessati

Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità alle norme di cui agli artt. da 15 a 22 del GDPR e, in particolare, quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento.

In riferimento alle immagini registrate non sono, in concreto, esercitabili i diritti di aggiornamento, rettificazione e integrazione dei dati personali, in considerazione della natura intrinseca dei dati raccolti ma vale la pena ricordare che l'interessato ha il diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge.

24Marzo2021_