INFORMATIVE TEMATICHE SEAC

Direttore Responsabile Giovanni Bort

Privacy

La protezione dei dati personali nell'ambito della videosorveglianza (2° parte)

29 OTTOBRE 2024 | N. 28

di Elena Pilastro

In questa informativa...

Facendo seguito alla precedente Informativa 24 ottobre 2024, n. 27, si prosegue l'esame della disciplina privacy nel contesto della videosorveglianza, alla luce delle Linee guida 3/2019, adottate dal Comitato europeo per la protezione dei dati (EDPB) il 29 gennaio 2020.

Come anticipato nella precedente Informativa ITS n. 27/2024, la **disciplina privacy applicabile nel contesto della videosorveglianza non è oggetto di disciplina** specifica né a livello europeo (Regolamento UE 2016/679), né a livello nazionale (Codice privacy e D.Lgs. n. 101/2018).

A fronte di tale vuoto normativo, il **Comitato europeo per la protezione dei dati (EDPB)** ha emanato le **Linee guida 3/2019**, allo scopo di fornire indicazioni sull'**applicazione del GDPR** in relazione al **trattamento di dati personali attraverso dispositivi video**, inclusa la videosorveglianza.

Si prosegue e conclude l'esame delle citate Linee guida, anche alla luce degli esempi proposti dall'EDPB.

Trattamenti riguardanti categorie particolari di dati

I sistemi di videosorveglianza **raccolgono enormi quantità di dati personali**, che possono rivelare dati di natura altamente personale e **categorie particolari di dati**, di cui all'art. 9, Regolamento UE 2016/679.

In virtù del principio di minimizzazione dei dati, il titolare del trattamento dovrebbe sempre cercare di **ridurre al minimo** il rischio di acquisire **filmati che rivelino dati sensibili**.

Tuttavia, **non sempre** la **videosorveglianza** è considerata un **trattamento di categorie particolari di dati**, come nel caso dell'esempio seguente.

A tale riguardo, si riportano gli esempi proposti dalle Linee guida.

ESEMPI

- *Un'attività di videosorveglianza che acquisisce le immagini di una chiesa non rientra di per sé nel campo di applicazione dell'articolo 9. Tuttavia, il titolare del trattamento deve effettuare una valutazione particolarmente attenta ai sensi dell'articolo 6, paragrafo 1, lettera f), con riguardo agli interessi della persona interessata, tenendo conto della natura dei dati nonché del rischio di acquisire altri dati sensibili (ulteriori rispetto a quelli di cui all'articolo 9).*
- *Le riprese video che mostrano un interessato che indossa occhiali o utilizza una sedia a rotelle non sono di per sé considerate categorie particolari di dati personali.*

Alcuni **dati raccolti tramite video**, apparentemente non significativi, possono essere **utilizzati per ricavare altre informazioni**, come ad esempio **categorie particolari di dati**, e raggiungere uno scopo diverso da quello iniziale (es. mappare le abitudini di un individuo).

Se le **riprese video** sono **trattate per ricavare categorie particolari di dati**, il **titolare** del trattamento **deve individuare** sia un'**eccezione**, ai sensi dell'**articolo 9, Regolamento UE 2016/679**, sia una **base giuridica**, ai sensi dell'**articolo 6, Regolamento UE 2016/679**, che consentano il trattamento di tali dati.

*Si noti che il semplice fatto di **entrare nell'area di ripresa della telecamera non implica che l'interessato intenda rendere pubbliche categorie particolari di dati** che lo riguardano; di conseguenza, il titolare del trattamento non potrà invocare la lettera e), paragrafo 2, art. 9, che consente il trattamento di dati personali resi manifestamente pubblici dall'interessato.*

Si riportano i seguenti esempi contenuti nelle Linee guida in esame.

ESEMPI

- *Sono acquisite le riprese video di un evento, uno sciopero o un corteo. Dalle immagini che mostrano gli interessati identificabili mentre partecipano a tali manifestazioni, si potrebbero, ad esempio, dedurre opinioni politiche. Questo caso rientrerebbe nell'ambito di applicazione dell'articolo 9, trattandosi si categorie particolari di dati.*
- *Un ospedale che installa una videocamera per monitorare le condizioni di salute di un paziente effettua un trattamento di categorie particolari di dati personali (articolo 9).*
- *Un datore di lavoro non deve utilizzare registrazioni di videosorveglianza che mostrano una manifestazione al fine di identificare gli scioperanti.*

Trattamento di dati biometrici

L'**uso della videosorveglianza** associata alla funzionalità del **riconoscimento biometrico** da parte di **soggetti privati per proprie finalità** (es. marketing, statistiche, sicurezza) richiede il **consenso** esplicito di tutti gli interessati, ai sensi dell'art. 9, paragrafo 2, lettera a), Regolamento UE 2016/679; potrebbe, tuttavia, essere applicabile anche un'altra deroga di cui all'articolo 9, Regolamento UE 2016/679.

Qualora il **trattamento biometrico** sia utilizzato a fini di **autenticazione** e sia richiesto il **consenso** ai sensi dell'articolo 9, Regolamento UE 2016/679, il **titolare** del trattamento **non deve condizionare l'accesso ai propri servizi all'accettazione del trattamento biometrico**; al contrario, il titolare deve offrire una **soluzione alternativa**, senza imporre restrizioni o costi aggiuntivi all'interessato.

*Le Linee guida sottolineano che, nei casi in cui vengano generati modelli biometrici, i **titolari** del trattamento sono tenuti a **garantire** che, una volta ottenuta una corrispondenza o non corrispondenza, tutti i **modelli intermedi realizzati in tempo reale** vengano **cancellati immediatamente e in modo sicuro**.*

Si vedano i seguenti esempi.

ESEMPI

- *Per migliorare il servizio, un'impresa privata sostituisce i posti di controllo per l'identificazione dei passeggeri all'interno di un aeroporto (consegna bagagli, imbarco) con sistemi di videosorveglianza che utilizzano tecniche di riconoscimento facciale per verificare l'identità dei passeggeri che hanno scelto di acconsentire a tale procedura. Poiché il trattamento rientra nel campo di applicazione dell'articolo 9, i passeggeri che avranno precedentemente prestato il consenso esplicito e informato dovranno registrarsi, ad esempio, presso un terminale automatico per creare e registrare il rispettivo modello facciale associato alla carta d'imbarco e al documento d'identità. I posti di controllo con riconoscimento facciale devono essere mantenuti chiaramente separati: ad esempio, il sistema deve essere installato all'interno di un varco di sicurezza, in modo da non acquisire i modelli biometrici delle persone che non hanno prestato il consenso. Solo i passeggeri che avranno preventivamente prestato il loro consenso e proceduto alla registrazione utilizzeranno il varco dotato del sistema biometrico.*

- *Un titolare del trattamento gestisce l'accesso al proprio edificio utilizzando un metodo di riconoscimento facciale. L'utilizzo di questa modalità di accesso è possibile solo se gli interessati hanno preventivamente prestato il loro consenso informato ed esplicito (ai sensi dell'articolo 9, paragrafo 2, lettera a). Tuttavia, al fine di garantire che non vengano acquisiti i dati di coloro che non abbiano precedentemente prestato il consenso, il riconoscimento facciale dovrebbe essere attivato dall'interessato stesso, ad esempio premendo un pulsante. Per assicurare la liceità del trattamento, il titolare deve sempre offrire una modalità alternativa di accesso all'edificio senza trattamento biometrico, ad esempio tramite badge o chiavi.*
- *Il proprietario di un esercizio commerciale vorrebbe personalizzare la propria pubblicità in base al genere e all'età dei clienti, acquisendo tali caratteristiche attraverso un sistema di videosorveglianza. Se tale sistema non genera modelli biometrici al fine di identificare in modo univoco le persone, ma semplicemente rileva tali caratteristiche fisiche al fine di classificare le persone, il trattamento non ricade nel campo di applicazione dell'articolo 9 (purché non siano trattate altre categorie particolari di dati).*
- *Un negoziante ha installato un sistema di riconoscimento facciale all'interno del proprio negozio al fine di personalizzare la pubblicità rivolta ai clienti. Il titolare del trattamento deve ottenere il consenso esplicito e informato di tutti gli interessati prima di utilizzare questo sistema biometrico e trasmettere pubblicità personalizzata. Il sistema sarebbe illegale se acquisisse i dati dei visitatori o dei passanti che non hanno acconsentito alla creazione di un modello biometrico, anche se quest'ultimo venisse eliminato nel più breve tempo possibile. Infatti, questi modelli temporanei costituiscono dati biometrici trattati al fine di identificare in modo univoco una persona che potrebbe non voler ricevere pubblicità mirata.*
- *Un hotel utilizza la videosorveglianza per avvisare automaticamente il direttore dell'arrivo di un VIP nel momento in cui il volto dell'ospite viene riconosciuto. I VIP in questione hanno prestato preventivamente il consenso esplicito all'uso del riconoscimento facciale, prima di essere registrati in una banca dati istituita a tale scopo. Questi sistemi di trattamento di dati biometrici sarebbero illegali, a meno che tutti gli altri ospiti monitorati (al fine di identificare i VIP) abbiano acconsentito al trattamento ai sensi dell'articolo 9, paragrafo 2, lettera a), del GDPR.*
- *Un titolare del trattamento installa un sistema di videosorveglianza con riconoscimento facciale all'ingresso della sala da concerti da lui gestita. Il titolare deve predisporre ingressi chiaramente separati: uno provvisto del sistema biometrico e uno senza (dove, ad esempio, si esegue la scansione di un biglietto). Gli ingressi dotati di dispositivi biometrici devono essere installati e resi accessibili in modo da impedire al sistema di acquisire modelli biometrici di spettatori non consenzienti.*

Diritti dell'interessato

Le Linee guida 3/2019 contengono una serie di chiarimenti in merito ad alcuni dei **diritti dell'interessato** sanciti dal GDPR, **declinati concretamente nell'ambito** di un trattamento dei dati associato all'impiego della **videosorveglianza**.

Diritto di accesso

Ai fini dell'esercizio del diritto di accesso, l'**interessato dovrebbe specificare quando** - entro un lasso di tempo ragionevole in proporzione alla quantità di interessati registrati - è **entrato nella zona sorvegliata**. Specularmente, il **titolare** dovrebbe notificare **preventivamente** all'interessato **di quali informazioni ha bisogno** per poter soddisfare la richiesta di accesso.

Si vedano i seguenti esempi.

ESEMPI

- *Qualora l'interessato richieda una copia dei propri dati personali trattati mediante videosorveglianza all'ingresso di un centro commerciale con 30.000 visitatori al giorno, deve specificare quando è entrato nella zona monitorata indicando una finestra di circa un'ora. Se il titolare del trattamento sta ancora trattando il materiale, dovrebbe fornirgli una copia del filmato. Se altri interessati possono essere identificati nello stesso materiale, allora quella parte del materiale deve essere anonimizzata (ad esempio sfocando la copia o parti di essa) prima che la copia sia consegnata all'interessato che ha presentato la richiesta.*
- *Se il titolare del trattamento cancella automaticamente tutte le riprese, ad esempio entro due giorni, non sarà in grado di fornire le riprese all'interessato dopo tale lasso di tempo. Se il titolare del trattamento riceve una richiesta successivamente, l'interessato dovrebbe esserne informato di conseguenza.*

Diritto alla cancellazione (diritto all'oblio)

Se il titolare del trattamento continua a trattare dati personali al di là del monitoraggio in tempo reale, l'interessato può chiederne la **cancellazione**.

Il titolare è tenuto a cancellare i dati personali **senza ingiustificato ritardo** (ai sensi dell'art. 17, par. 1, Regolamento UE 2016/679) e dovrebbe, altresì, **informare qualunque soggetto al quale siano stati precedentemente comunicati** tali **dati** (art. 19, Regolamento UE 2016/679).

*Le Linee guida chiariscono che, **offuscando l'immagine senza** alcuna **possibilità di recuperare** successivamente i **dati personali** precedentemente nell'immagine stessa, si deve ritenere che i dati personali siano stati **cancellati** in conformità delle disposizioni del GDPR.*

ESEMPIO

Un minimarket ha subito atti vandalici, in particolare sull'esterno del negozio, e utilizza quindi la videosorveglianza al di fuori dell'entrata, con la telecamera che riprende l'area prossima alle pareti. Un passante chiede che vengano cancellati i suoi dati personali a partire da quel momento. Il titolare del trattamento è tenuto a rispondere alla richiesta senza ingiustificato ritardo e al più tardi entro un mese. Poiché il filmato in questione non soddisfa più lo scopo per il quale è stato inizialmente conservato (non si è verificato alcun atto vandalico durante il periodo in cui l'interessato è transitato nei pressi del negozio), al momento della richiesta non vi è alcun interesse legittimo a conservare i dati tale da prevalere sugli interessi degli interessati. Il titolare del trattamento deve cancellare i dati personali.

Diritto di opposizione

Se l'**interessato si oppone alla sorveglianza**, ai sensi dell'**articolo 21, Regolamento UE 2016/679**, il trattamento dei dati della persona che vi si è opposta deve cessare, **salvo** che il titolare dimostri l'**esistenza di motivi legittimi cogenti** che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato.

Nel contesto della videosorveglianza, l'**opposizione** può essere formulata **all'ingresso, durante il periodo di permanenza nella zona sorvegliata o dopo l'uscita** dalla stessa.

*Nel caso in cui si utilizzi la **videosorveglianza per finalità di marketing diretto**, il **diritto di opposizione** è **assoluto**; di conseguenza, l'interessato ha diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità (art. 21, paragrafi 2 e 3, Regolamento UE 2016/679).*

Si riporta di seguito l'esempio proposto dalle Linee guida.

ESEMPIO

Un'impresa sta incontrando difficoltà a causa di violazioni della sicurezza che si verificano all'ingresso riservato al pubblico e utilizza la videosorveglianza per motivi di legittimo interesse, allo scopo di individuare coloro che entrano illegalmente. Un visitatore si oppone al trattamento dei propri dati attraverso il sistema di videosorveglianza per motivi connessi alla sua situazione particolare. In questo caso, tuttavia, l'impresa respinge la richiesta spiegando che le riprese conservate sono necessarie in quanto è in corso un'indagine interna, motivo legittimo cogente per continuare a trattare i dati personali.

Obblighi di trasparenza e informazione

Le Linee guida in esame precisano che, se i **dati personali** sono **raccolti** presso l'interessato **mediante osservazione** (es. utilizzando dispositivi o software per catturare dati in modo automatizzato, quali **telecamere**), trova applicazione l'**articolo 13, Regolamento UE 2016/679**.
Gli **interessati** devono essere **consapevoli** del fatto che è in funzione un **sistema di videosorveglianza** e dovrebbero, inoltre, essere **informati in modo dettagliato sui luoghi sorvegliati**.
A tal fine, i titolari del trattamento possono seguire un **approccio informativo scalare**:

- le **informazioni più importanti** devono essere indicate sul **segnale di avvertimento** (c.d. informazioni di **primo livello**);
- gli **ulteriori dettagli obbligatori** possono essere forniti con altri mezzi (c.d. informazioni di **secondo livello**).

Informazioni di primo livello

Nella prima fase di interazione tra il titolare del trattamento e l'interessato, il titolare può utilizzare un **segnale di avvertimento** che indichi le **informazioni che consentano all'interessato di riconoscere** facilmente le **circostanze della sorveglianza**; tali informazioni possono essere fornite **in combinazione con un'icona standardizzata**, così da fornire, in modo ben visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto (art. 12, paragrafo 7, Regolamento UE 2016/679).

*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 stimare quale zona sia coperta da una telecamera in modo da evitare la sorveglianza o adeguare il proprio comportamento, ove necessario.*

Le informazioni di primo livello dovrebbero comunicare i **dati più importanti**, quali ad esempio:

- le **finalità** del trattamento;
- l'**identità del titolare** del trattamento;
- l'esistenza di **diritti dell'interessato**;
- gli **impatti** più consistenti del **trattamento** sui diritti dell'interessato.

L'informativa di primo livello dovrebbe anche **rinviare alle informazioni di secondo livello**, in quanto maggiormente dettagliate, indicando **come e dove trovarle**; a tal fine, è preferibile che si faccia riferimento a una **fonte digitale** (es. codice QR o indirizzo web).

*La segnaletica deve contenere anche le **informazioni** che potrebbero risultare **inaspettate per l'interessato**, come ad esempio la **trasmissione di dati a terzi** (soprattutto se ubicati al di fuori dell'UE) e il **periodo di conservazione**; se tali informazioni **non** sono **indicate**, l'interessato dovrebbe confidare nel fatto che vi sia **solo** una **sorveglianza in tempo reale**, senza alcuna registrazione di dati o trasmissione a soggetti terzi.*

L'informativa può essere fornita utilizzando un **modello semplificato**, come quello **realizzato dall'EDPB**.

Informazioni di secondo livello

Le informazioni di secondo livello devono contenere tutti gli **elementi obbligatori** a norma dell'**articolo 13, Regolamento UE 2016/679**.

Tali informazioni devono essere **facilmente accessibili per l'interessato**, ad esempio attraverso un pagina informativa completa messa a disposizione in uno snodo centrale (es. sportello informazioni, reception, cassa, ecc.) o affissa in un luogo di facile accesso.

Nonostante sia preferibile che nelle informazioni di primo livello vi sia il riferimento ad una **fonte digitale**, le informazioni di secondo livello dovrebbero essere facilmente disponibili anche in **formato non digitale**.

*Dovrebbe essere possibile accedere al secondo livello di informazioni **senza entrare nell'area videosorvegliata**, soprattutto se le informazioni sono fornite digitalmente.*

Le Linee guida propongono il seguente esempio.

ESEMPIO

Un negoziante videosorveglia il suo esercizio commerciale. Ai fini del rispetto delle disposizioni dell'articolo 13, GDPR, è sufficiente che collochi un cartello di avvertimento in un punto facilmente visibile all'ingresso dell'esercizio commerciale, contenente le informazioni di primo livello. Dovrà poi fornire le informazioni di secondo livello attraverso un foglio informativo disponibile presso la cassa o qualsiasi altro punto centrale e facilmente accessibile all'interno dell'esercizio.

Conservazione e obbligo di cancellazione delle immagini registrate

I dati personali **non** possono essere **conservati più a lungo di quanto necessario per le finalità** per le quali sono trattati (art. 5, paragrafo 1, lettere c) e e), Regolamento UE 2016/679.

Gli **Stati membri** possono prevedere **disposizioni specifiche** per i periodi di conservazione con riguardo alla videosorveglianza, a norma dell'art. 6, paragrafo 2, Regolamento UE 2016/679.

Spetta al **titolare** del trattamento **definire il periodo di conservazione** con riguardo alle singole finalità, nonché conformemente ai principi di necessità e proporzionalità e alle disposizioni del Regolamento.

*Il titolare del trattamento deve valutare la **necessità** o meno di **conservare i dati personali** entro una **tempistica ristretta**.*
*Nella maggior parte dei casi, i dati personali dovrebbero essere **cancellati dopo alcuni giorni**, preferibilmente tramite **meccanismi automatici**.*

Di seguito si riporta l'esempio proposto dalle Linee guida in esame.

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. Se viene rilevato un danno, può essere anche necessario conservare il filmato per un periodo più lungo al fine di intraprendere un'azione legale contro l'autore del reato.

Misure tecniche e organizzative

Ai sensi dell'articolo 32, paragrafo 1, Regolamento UE 2016/679, il **titolare** ed il **responsabile** del trattamento devono garantire l'**adeguata sicurezza dei dati** in tutte le fasi, ossia durante la **conservazione** (dati a riposo), la **trasmissione** (dati in transito) ed il **trattamento** (dati in uso).

A tal fine, i titolari del trattamento devono mettere in atto **adeguate misure tecniche ed organizzative** sia nella fase di **progettazione del sistema di videosorveglianza**, sia all'atto del **trattamento** stesso (ai sensi degli articoli 24 e 25, Regolamento UE 2016/679).

*Le **misure tecniche ed organizzative** attuate devono essere **proporzionate ai rischi per i diritti e le libertà delle persone fisiche** derivanti dai casi di distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso ai dati di videosorveglianza.*

Nel selezionare le soluzioni tecniche, il titolare del trattamento dovrebbe considerare le **tecnologie che tutelano la privacy**, come ad esempio i sistemi che consentono il **mascheramento** o l'**offuscamento** delle **zone irrilevanti** per la sorveglianza oppure l'**editing** di **immagini di terzi** quando si forniscono filmati agli interessati. Le ulteriori **funzioni** fornite, ma **non necessarie**, dovrebbero essere **disattivate** (es. movimento illimitato delle telecamere, capacità di zoom, radiotrasmissione, analisi e registrazioni audio).

Valutazione d'impatto sulla protezione dei dati

Ai sensi dell'articolo 35, paragrafo 1, Regolamento UE 2016/679, i **titolari** del trattamento sono tenuti a condurre una **valutazione di impatto sulla protezione dei dati** quando una determinata tipologia di trattamenti può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**.

In particolare, i titolari sono tenuti ad effettuare valutazioni di impatto sulla protezione dei dati:

- se il trattamento consiste nella **sorveglianza sistematica di una zona accessibile al pubblico su larga scala**;
- quando il titolare intende **trattare categorie particolari di dati su larga scala**.

Ogni **autorità di controllo** pubblica un **elenco** delle **tipologie di trattamento soggette obbligatoriamente a valutazioni di impatto** sulla protezione dai dati nel rispettivo Stato membro (art. 35, paragrafo 4, Regolamento UE 2016/679).

L'esito della valutazione di impatto sulla protezione dei dati dovrebbe determinare la **scelta** del titolare del trattamento sulle **misure di protezione dei dati** implementate.

Ove i risultati della valutazione di impatto sulla protezione dei dati indichino che il trattamento comportebbe un **rischio elevato nonostante le misure di sicurezza** pianificate dal titolare, occorre **consultare** l'**autorità di controllo** competente prima di procedere al trattamento.