GDPR: Linee guida per la videosorveglianza.
Di Valentino Vescio di Martirano.

Sono state rese note dall'*European Data Protection Board* (EDPB) le linee guida 3/2019 del 12 luglio 2019 sul trattamento dei dati personali in merito ai servizi di videosorveglianza.
Le linee guida in commento sono interessanti perché l'utilizzo intensivo dei sistemi di video sorveglianza ha modificato il comportamento dei cittadini che, sentendosi osservati, modificano il loro atteggiamento, diverso da quello che avrebbero avuto nel caso fossero rimasti anonimi.
Le linee guida si prefiggono lo scopo di fornire gli strumenti utili per evitare che la legittima acquisizione di video registrazioni scivoli poi in un trattamento illecito o non conforme al GDPR.
Di seguito una rielaborazione di quanto descritto nelle linee guida 3/2019.

1. L'analisi del trattamento dati nei casi di Videosorveglianza a mente dell'Articolo 5 GDPR.

Per identificare le finalità del trattamento si deve verificare quanto prescritto dall'Articolo 5 del GDPR.
Invero, le finalità possono cambiare a seconda che il **titolare** sia **pubblico** o **privato**, che la video sorveglianza abbia la finalità di migliorare la sicurezza, per fornire strumenti di pubblicità mirata.
A volte poi le tecniche di video sorveglianza hanno carattere altamente intrusivo (es. tecnologie biometriche complesse) o meno intrusive (ad esempio semplici algoritmi di conteggio delle persone in un locale).
Sul punto l'EDPB fa notare come gli algoritmi spesso non siano totalmente affidabili e che i titolari e responsabili della videosorveglianza devono mantenere un grado minimo di affidabilità dei sistemi di video sorveglianza per evitare scelte giuridiche affidate a tali sistemi (come l'identificazione facciale o il riconoscimento) abbia risultati errati e quindi deleteri.
Inoltre l'EDPB afferma che la videosorveglianza non è l'unico strumento da adottare per alcune finalità perseguite dal titolare del trattamento.

2. L'area di applicazione del GDPR nel trattamento dei dati nella video sorveglianza.

2.1 I Dati personali raccolti

È di tutta evidenza che una volta entrato in un locale videosorvegliato, si raccolgono così tante immagini e video correlate ad un interessato.
La raccolta di tutte le informazioni relative alle persone monitorate consente l'elaborazione di dati personali riferibili alla presenza della persona in un determinato luogo e permette di valutarne il comportamento o estrapolarne dettagli che a prima vista non sarebbero percepibili ad occhio nudo.
L'abuso che potrebbe derivarne da tali informazioni è evidente.
Più è ampia la sorveglianza più è alto il rischio.
Sul punto basti evidenziare che l'articolo 35, paragrafo 3, lettera c) del GDPR prescrive la DPIA in caso di monitoraggio sistematico su larga scala di un'area accessibile al pubblico (si veda il paragrafo 10 in calce).
Inoltre è degno di nota quanto prescritto all'articolo 37, paragrafo 1, lettera b) GDPR che in questi casi impone la nomina di un **DPO**.
Tuttavia, il GDPR non si applica quando la persona non è in alcun modo identificabile, direttamente o indirettamente.
Qui di seguito gli esempi forniti dall'EDPB in cui non si applica il GDPR:
a) **telecamere false** (cioè quelle che non registrano video o immagini) poiché non vengono elaborati dati personali;

b) **video registrazioni ad alta** quota (perché le immagini non possono essere agganciate ad un soggetto preciso);
c) **videocamera a bassa risoluzione**, non in grado di raccogliere alcuna informazione relativa ad una specifica persona fisica (come targhe o informazioni che potrebbero identificare i passanti).

2.2 Direttiva EU2 016/680

Ogni trattamento dei dati personali (anche da video registrazione) da parte delle autorità competenti ai fini della prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, non è disciplinato dal GDPR ma dalla Direttiva EU 2016/680

2.3 Eccezioni per fini domestici

Ai sensi dell'articolo 2, paragrafo 2, lettera c), il trattamento di dati personali da parte di una persona fisica nel corso di attività puramente personali o domestiche, che possono includere anche attività *online*, è da considerarsi fuori dal campo di applicazione del GDPR (si veda anche il considerando n.18).
Questa eccezione – specie nel contesto della videosorveglianza - deve essere interpretato restrittivamente.
Sul punto, la Corte di Giustizia (sentenza nella causa C-101/01, *caso Bodil Lindqvist* , 6 novembre 2003, paragrafo 47) afferma che tale eccezione si riferisce solo alle attività svolte nel corso della vita privata o familiare, e tale non può essere la condivisione su Internet di tali dati, che di conseguenza sono resi accessibili a un numero indefinito di persone.
Inoltre, se un sistema di videosorveglianza registra ed archivia immagini, anche parzialmente, di uno spazio pubblico*,* non può più essere considerata tale attività come privata o familiare (Corte di giustizia europea, sentenza nella causa C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů* , 11 dicembre 2014, par. 33.)

Esempio: un turista sta registrando un video sia attraverso il suo telefono cellulare che attraverso una videocamera per documentare le sue vacanze.
Mostra il filmato ad amici e parenti ma non lo rende accessibile ad un numero indefinito di persone. Questo ricadrebbe nell'eccezione richiamata.

Esempio: un *mountainbiker* vuole registrare la sua discesa con una *actioncam*. Le registrazioni verranno visionate per il suo intrattenimento. Anche questa circostanza ricade nell'eccezione.

Esempio: qualcuno ha installato un sistema di video sorveglianza nel proprio giardino.
La proprietà è recintata e solo il titolare stesso e la sua famiglia hanno accesso regolarmente nel giardino. Questo rientrerebbe nell'eccezione a condizione che la videosorveglianza non monitori, anche parzialmente, uno spazio pubblico o una proprietà altrui.

3 LEGITTIMITÀ DEL TRATTAMENTO

Prima di ogni trattamento effettuato con dispositivi video devono essere specificate nel dettaglio le sue finalità (Articolo 5, paragrafo 1, lettera b), GDPR).
Le finalità della video sorveglianza possono essere diverse:
- la protezione della proprietà e di altri beni;
- la raccolta di prove per il diritto di difesa nei processi civili.

Per questa ragione, le finalità devono
- essere documentate per iscritto (articolo 5, paragrafo 2, GDPR);
- essere specifiche per ogni sistema di video sorveglianza in uso (cioè raggruppate per scopi comuni);

- devono fornire informazioni agli interessati in modo da far comprendere le finalità e gli scopi del trattamento conformemente all'articolo 13 del GDPR.

Secondo l'EDPB la semplice finalità per fini di "sicurezza" non è sufficientemente specificata poiché non si aggancia alle diverse base giuridiche di cui all'art. 6.

3.1 Le basi giuridiche

Ad esempio, si applica l'articolo 6, paragrafo 1, lettera c), GDPR quando è la stessa legge a prevedere l'obbligo di video sorveglianza.

Comunque le basi giuridiche più comuni sono quelle fondate:

- sull'Articolo 6, paragrafo 1, lettera f), GDPR (**legittimo interesse**).
- sull'Articolo 6, paragrafo 1, lettera e), GDPR (necessità di svolgere un compito svolto **nell'interesse pubblico** o **nell'esercizio di autorità ufficiale**)
- sull'Articolo 6, paragrafo 1, lettera a), GDPR (**consenso**).

3.1.1 Legittimo interesse

La videosorveglianza è lecita se è necessaria a soddisfare la finalità per legittimo interesse perseguito da un titolare del trattamento o da terzi, a meno che tali interessi non mettano a rischio i diritti e libertà fondamentali dell'interessato (articolo 6, paragrafo 1, lettera f), GDPR).

Per legittimo interesse si intende un interesse:

a) **legale**;
b) **economico**;
c) **immateriale**.

Tuttavia, l'interessato può opporsi (ai sensi dell'art. 21 GDPR) al trattamento dei dati (anche per i sistemi di videosorveglianza) e ciononostante il titolare può procedere con la videosorveglianza laddove il legittimo interesse prevalga sugli interessi, i diritti e le libertà dell'interessato o per esercitare il diritto di difesa.

Invero, in una situazione realmente pericolosa, la finalità di proteggere la proprietà ad es. da un furto può costituire un legittimo interesse per giustificare la videosorveglianza.

Il legittimo interesse deve essere pertanto:

- **reale** (cioè non deve essere immaginario o speculativo); e,
- **attuale** (cioè non potenziale ma concreto, ad esempio una situazione di pericolo imminente può costituire una base giuridica da legittimo interesse; ad esempio le gioiellerie o le stazioni di benzina).

Del pari il legittimo interesse non può essere desunto in *re ipsa* ma deve essere valutato caso per caso e bilanciato con i diritti dell'interessato.

3.1.2 Necessità del trattamento.

I dati personali devono essere **adeguati**, **pertinenti** e **limitati** in relazione alle finalità per i quali sono trattati ("**minimizzazione dei dati**"), a mente dell'Articolo 5, paragrafo 1, lettera c), GDPR.

Prima di installare un sistema di videosorveglianza il titolare dovrebbe verificare che tale misura è proporzionata alla finalità perseguita.

Invero la videosorveglianza dovrebbe essere adottata come *extrema ratio*.

Ad esempio, l'EDPB suggerisce che se la finalità è quella di prevenire i reati connessi alla proprietà, invece di installare un sistema di videosorveglianza, il titolare potrebbe anche adottare misure di sicurezza alternative come sistemi di sorveglianza quali assumere personale di sicurezza.

Esempio: il proprietario di un negozio desidera aprire un nuovo esercizio commerciale e desidera installare una sistema di videosorveglianza. A base del legittimo interesse, egli può riferirsi alle statistiche di atti di vandalismo in quel quartiere o riferirsi ad esperienze dei locali commerciali dei negozi vicini.
Tuttavia, non è sufficiente per giustificare un legittimo interesse basarsi su statistiche nazionali o generali senza analizzare l'area in questione o i pericoli specifici inerenti il negozio.

Inoltre, secondo l'EDPB, prima di installare un sistema di video sorveglianza il titolare è obbligato a valutare dove e quando le telecamere di sorveglianza sono strettamente necessarie (per esempio di notte e situate nel perimetro della proprietà).

Esempio: una libreria vuole proteggere i suoi locali contro atti di vandalismo.
In generale, le fotocamere dovrebbero solo filmare i locali interni perché non è necessario installare telecamere nei luoghi attigui o aree pubbliche nelle vicinanze.

Pertanto, per minimizzare i dati e per evitare una eccessiva raccolta, viene spesso utilizzato il *black box* in cui il filmato viene automaticamente eliminato dopo un certo periodo di archiviazione e accessibile solo in caso di incidente.

3.1.3 Bilanciamento degli interessi

Dando per assodato che la videosorveglianza sia necessaria per proteggere i legittimi interessi di un titolare, come detto è necessario sempre **bilanciare gli interessi** contrapposti dell'interessato.
In particolare, il titolare deve considerare:
1) in che misura il monitoraggio incide sugli interessi, diritti fondamentali e le libertà degli individui; e
2) se ciò provochi violazioni o conseguenze negative sui diritti dell'interessato.

Tale bilanciamento di interessi è obbligatorio:
da una parte, i diritti fondamentali e libertà dell'interessato; dall'altra, gli interessi legittimi del titolare.

Esempio: una società di parcheggi ha documentato il ripetersi di episodi di furto delle macchine parcheggiate. L'area di parcheggio è uno spazio aperto e può essere facilmente accessibile da chiunque, seppur debitamente segnalato con cartelli che circondano il perimetro.
Il legittimo interesse è prevenire i furti delle auto dei clienti.
Dall'altro gli interessati hanno diritto a non essere monitorati, nonostante che la videoregistrazione avvenga per la prevenzione dei furti e sia effettuata anche a loro vantaggio. Quindi il monitoraggio è limitato solo alla sorveglianza delle auto ma non alla sorveglianza degli stessi clienti.

Esempio: un ristorante decide di installare delle videocamere nei servizi igienici per controllare la loro pulizia. In questo caso i diritti degli interessati hanno chiaramente la precedenza sul legittimo interesse del titolare, quindi le telecamere non possono essere installate nei servizi igienici.

3.1.3.1 Bilanciamento case-by-case

Seguendo l'impostazione data dall'Articolo 6, paragrafo 1, lettera f), GDPR, il bilanciamento degli interessi è obbligatorio e deve essere concreto ed attuale (quindi non formale).
Il titolare, ad esempio, deve valutare il peso (numero dei dati e delle persone o le dimensioni dell'area monitorata) ed i rischi dei diritti e delle libertà degli interessati coinvolti; nonché la possibilità di disporre di valide alternative alla videosorveglianza.

Esempio: se viene installata una *dash cam* (ad es. per raccogliere eventualmente prove nel caso di un incidente), è importante assicurarsi che anche questa telecamera non stia registrando costantemente le persone presenti sulla strada. Altrimenti la finalità andrebbe fuori dal perimetro del legittimo interesse alla video registrazione e cioè si trasformerebbe nella finalità di monitorare i dati di terzi in generale.

3.1.3.2 Ragionevoli aspettative degli interessati

Secondo il considerando 47 del GDPR, l'esistenza di un legittimo interesse richiede un'attenta valutazione anche delle aspettative degli interessati, per tale intendendosi l'aspettativa dell'interessato ad essere tutelato dal titolare nella valutazione del caso concreto.
Ad esempio, un dipendente sul posto di lavoro nella maggior parte dei casi non si aspetta che sia monitorato dal suo datore di lavoro.
Allo stesso modo, non è ragionevole aspettarsi di essere monitorati in strutture sanitarie o altre aree che per definizione sono riconosciute come zone private.

Esempio: nei servizi igienici ci si aspetta di non essere monitorati.

Di contro, il cliente di una banca potrebbe aspettarsi che venga monitorato all'interno della stessa banca.

L'aspettativa di essere monitorati può esserci anche nei luoghi pubblici, dove il legittimo interesse è declinazione **dell'Articolo 6, paragrafo 1, lettera e), GDPR**, per svolgere quelle attività nell'interesse pubblico (come salute e sicurezza per la protezione di dipendenti e visitatori).

3.3 Base giuridica tramite consenso ai sensi dell'Articolo 6, paragrafo 1, lettera a), GDPR.

Come noto il consenso deve essere
a) **libero**;
b) **specifico**;
c) **informato**;
d) **attuale**;
e) **revocabile**.
Tali presupposti si applicano anche alla videosorveglianza, con la precisazione che il consenso può costituire valida base giuridica solo in casi eccezionali a mente dell'Articolo7 GDPR (cfr. considerando 43).
Infatti, per sua natura la videosorveglianza consente di monitorare contemporaneamente un numero sconosciuto di persone.
Il titolare difficilmente sarà in grado di provare che l'interessato abbia dato il proprio consenso prima del trattamento dei propri dati personali (Articolo 7, paragrafo 1, GDPR).
Come del resto sarebbe difficile che in caso di revoca del consenso, il titolare sia in grado di non trattare più quei dati riferibili a quel singolo interessato (Articolo 7, paragrafo 3, GDPR).
Tuttavia, se il titolare intende giovarsi della base giuridica del consenso, è suo dovere assicurarsi che ogni persona interessata conferisca il suo esplicito consenso (per esempio quando si attraversa un'area particolare come un corridoio o un cancello specifico per entrare in un luogo monitorato).
Oppure, nel caso di videosorveglianza nei luoghi di lavoro, ove dato lo squilibrio di potere tra datore di lavoro e dipendenti, nella maggior parte dei casi i datori di lavoro dovrebbero non fare affidamento sul consenso, in quanto è improbabile che venga dato liberamente (sul punto si rimanda a quanto previsto dall'art. 4 dello Statuto dei lavoratori).

Esempio: gli atleti possono richiedere di essere monitorati durante le singole esercitazioni per analizzarne le proprie tecniche e prestazioni. Tuttavia, se un *club* sportivo prende l'iniziativa di monitorare un'intera squadra per la medesima finalità, il consenso spesso non è valido poiché il singolo atleta o gli atleti possono sentirsi costretti a dare il consenso per evitare che il loro rifiuto possa influire negativamente, anche sugli stessi compagni di squadra.

4 Divulgazione di filmati a terzi

In linea di principio, il GDPR disciplina i casi di divulgazione di registrazioni video a terzi.

4.1 Divulgazione di riprese video a terzi in generale

La divulgazione come "trattamento dati" è definita all'articolo 4, paragrafo 2, GDPR, come trasmissione (ad es. comunicazione individuale), diffusione (ad esempio, la pubblicazione online) o la messa a disposizione in altro modo.
I terzi sono definiti all'articolo 4, paragrafo 10, GDPR (inoltre, il WP Group 29 ha adottato delle specifiche linee guida al riguardo).
Ad ogni modo, qualsiasi divulgazione di filmati contenenti dati personali deve avere una specifica base giuridica (Articolo 6, paragrafo 4, GDPR).

Esempio: un titolare che desideri caricare una registrazione su Internet deve fare affidamento su una base giuridica per tale trattamento, ad esempio ottenendo il consenso dell'interessato secondo Articolo 6, paragrafo 1, lettera a), GDPR.

La stessa valutazione deve essere effettuata dal destinatario che, in particolare, dovrà identificare la sua base giuridica ai sensi dell'Articolo 6 (ad esempio la ricezione del materiale).

Esempio: il sistema di videosorveglianza posto su una barriera all'ingresso di un parcheggio è stata installata con lo scopo di risolvere eventuali richieste di risarcimento danni. Si verifica un danno e la registrazione viene trasferita ad un avvocato per seguirne il caso.
In questo caso la finalità della registrazione è il trasferimento del dato personale contenuto nella registrazione.
Laddove nella medesima situazione, però, la registrazione venisse pubblicata *online* per puro divertimento, in questo caso la finalità sarebbe diversa e non sarebbe compatibile con la finalità iniziale. Inoltre sarebbe problematico identificare una base giuridica per tale trattamento (pubblicazione) e si potrebbe immaginare il consenso dell'interessato.

4.2 Divulgazione di filmati alle forze dell'ordine

Anche la divulgazione di registrazioni video verso le forze dell'ordine è un trattamento separato che richiede una base giuridica diversa ai sensi dell'Articolo 6, paragrafo 1, lettera c), GDPR, per esempio per cooperare durante le indagini.

Esempio: un proprietario del negozio registra filmati al suo ingresso. Registra una persona che ruba un portafoglio. La polizia chiede al titolare di consegnare il materiale per finalità di indagine ai sensi dell'Articolo 6, paragrafo 1, lettera c), GDPR.

Esempio: una telecamera è installata in un negozio per motivi di sicurezza. Il proprietario del negozio crede di aver registrato qualcosa di sospetto e decide di inviare il materiale alla polizia (senza alcuna indicazione di una qualsivoglia indagine in corso). In questo caso il proprietario del negozio deve valutare se le condizioni di cui all'Articolo 6, paragrafo 1, lettera f), GDPR sono soddisfatte.

Ricordiamo che il trattamento dei dati personali da parte delle forze dell'ordine è disciplinato dalla direttiva EU 2016/680.

5 Trattamento delle categorie speciali di dati

I sistemi di videosorveglianza solitamente raccolgono enormi quantità di dati personali che possono rivelare dati natura strettamente personale e persino dati "particolari".
Dati apparentemente non significativi possono rivelare ad es. le abitudini di un individuo.

Non sempre, però, vengono trattati dati particolari.

Esempio: le riprese video che mostrano un soggetto con gli occhiali o una sedia a rotelle non possono essere considerati per sé come dati personali particolari.

Se la video sorveglianza tratta dati particolari, tale trattamento deve essere effettuato ai sensi dell'art. 9 GDPR e prim'ancora dovrebbe minimizzarsi il rischio di catturare filmati che rivelino altri dati sensibili, indipendentemente dalla finalità perseguita.

Esempio: le opinioni politiche potrebbero per esempio essere carpite da immagini che mostrano persone identificabili che prendono parte a un evento, impegnandosi in uno sciopero, ecc. Ciò ricadrebbe nell'alveo dell'Articolo 9 cit..

Esempio: un ospedale che installa una videocamera per monitorare le condizioni di salute del paziente sarebbe considerato come trattamento di categorie particolari di dati personali (Articolo 9 cit.).

Esempio: la videosorveglianza che monitora una chiesa non rientra di per sé nel perimetro dell'Articolo 9 cit.. Tuttavia, il titolare deve effettuare una valutazione particolarmente attenta ai sensi dell'articolo 6, paragrafo 1, lettera f) GDPR e verificare la natura dei dati e del rischio di essere acquisiti da altri come dati sensibili.

Se un sistema di videosorveglianza tratta dati particolari, il titolare dovrebbe porre a base giuridica quanto disposto dall'Articolo 9, paragrafo 2, lettera c), GDPR, secondo cui il trattamento è necessario per proteggere gli interessi vitali dell'interessato o di un'altra persona incapace di fornire il proprio consenso.
Tale base giuridica deve essere assoluta e necessaria per salvaguardare gli interessi vitali di una persona e non sono ammesse altre finalità.

Esempio: un ospedale sta monitorando un paziente per ragioni mediche. L'interessato è stato trasferito in ambulanza presso l'ospedale mentre era svenuto. In questo caso si potrebbe applicare l'articolo 9, paragrafo 2, lettera c), GDPR.

È importante notare che le deroghe elencate all'Articolo 9 GDPR non possono essere utilizzate per giustificare trattamenti ulteriori non leciti.
Inoltre, tale trattamento di dati particolari presuppone una vigilanza intensificata e continua, con alti livelli di sicurezza e con la preventiva valutazione dell'impatto sulla protezione dei dati degli interessati ove ciò si renda necessario.

Esempio: un datore di lavoro non deve utilizzare le registrazioni video che mostrano alcuni scioperanti in una manifestazione e ciò al fine non consentito di identificarli.

5.1 Considerazioni generali sul trattamento dei dati biometrici

L'uso di **dati biometrici** e in particolare il riconoscimento facciale comportano rischi elevati per i diritti degli interessati.
Il ricorso a tali tecnologie deve avvenire nel dovuto rispetto dei principi di **liceità**, **necessità**, **proporzionalità** e **minimizzazione** dei dati come stabilito nel GDPR.
Come detto è necessario effettuare una DPIA, specie per i dati biometrici, come ad esempio il fisico, caratteristiche fisiologiche o comportamentali di una persona.

Il GDPR afferma all'Articolo 4.14 che il dato biometrico deriva da un trattamento tecnico specifico relativo a **caratteristiche fisiche, fisiologiche o comportamentali**.
Un video di per sé non un dato biometrico ai sensi dell'Articolo 9 GDPR, se non è stato specificamente trattato tecnicamente al fine di contribuire all'identificazione di un individuo.
Affinché venga considerato come dato biometrico è necessario che il dato venga trattato allo **scopo di identificare in modo univoco una persona fisica**.
Dal combinato disposto degli Artt. 4.14 e 9, si possono considerare tre criteri per verificare se ci si trovi di fronte ad un dato biometrico:

-natura dei dati: dati relativi a caratteristiche fisiche, fisiologiche o comportamentali di una persona;

-mezzi e modalità di trattamento: cioè sono dati risultanti da un trattamento tecnico specifico;

-finalità del trattamento: la finalità del trattamento è quella di identificare univocamente una persona.

L'uso privato del riconoscimento biometrico tramite videosorveglianza (ad esempio per finalità di *marketing*, statistiche o di sicurezza) presuppone spesso come base giuridica un esplicito consenso di tutti gli interessati (articolo 9, paragrafo 2, lettera a) GDPR), con le relative eccezioni.

Esempio: per migliorare il suo servizio, un'azienda privata sostituisce all'interno di un aeroporto (deposito bagagli, imbarco) il controllo sull'identità del passeggero con un sistema di videosorveglianza che utilizza tecniche di riconoscimento facciale per verificarne l'identità dei passeggeri che rilasciato il loro consenso a tale procedura.
I passeggeri che hanno rilasciato precedentemente il loro consenso esplicito e informato, dovranno recarsi in una sezione separata dell'aeroporto affinché il riconoscimento facciale non sia associato ad altri passeggeri non consenzienti.

Esempio: un titolare gestisce l'accesso ad un edificio tramite riconoscimento facciale.
Solo le persone che hanno dato il consenso esplicitamente e preventivamente possono essere sottoposte a tale riconoscimento.
Per evitare che il riconoscimento facciale avvenga anche nei confronti di chi non ha rilasciato il proprio consenso, il sistema di riconoscimento facciale dovrebbe essere attivato dalla persona stessa che lo attiva tramite, ad esempio, un pulsante.
Inoltre, il titolare è tenuto a fornire un sistema alternativo per accedere all'edificio, senza pretendere in ogni caso la raccolta di dati biometrici, come *badge* o chiavi.

In questo tipo di casi, in cui vengono generati modelli biometrici, i titolari assicurano che una volta ottenuto il dato biometrico per la finalità perseguita ed con la base giuridica richiesta (ad es. il consenso), il dato dovrebbe essere immediatamente e in modo sicuro cancellato e non dovrebbe essere archiviato o conservato.

Inoltre, quando la finalità del trattamento è ad esempio quella di distinguere una categoria di persone da un'altra, ma non per identificare in modo univoco nessuno, il trattamento non rientra nel perimetro delineato dall'Articolo 9 GDPR.

Esempio: il proprietario di un negozio desidera personalizzare la propria pubblicità in base al genere e all'età del cliente tramite un sistema di videosorveglianza. Se il sistema biometrico non identifica in modo univoco le persone ma invece rileva solo le caratteristiche fisiche prescelte, allora il trattamento non rientra tra le categoria di dati descritti dall'Articolo 9 GDPR.

E' altrettanto vero però che l'Articolo 9 GDPR si applica se il titolare memorizza i dati biometrici e tali dati sono raccolti per indentificare una persona, anche per finalità di *marketing*.

Esempio: il proprietario di un negozio ha installato un sistema di riconoscimento facciale all'interno del suo negozio al fine di personalizzare la sua pubblicità nei confronti dei clienti. Il titolare si premura di ottenere preliminarmente il loro consenso. Il sistema sarebbe illecito se catturasse dati biometrici dei visitatori o passanti senza il loro consenso, anche se i loro dati venissero cancellati immediatamente dopo loro la loro acquisizione.

L'EDPB osserva che alcuni sistemi biometrici sono installati in un ambiente non controllato, cioè in un ambiente dove in maniera incontrollata viene fatto il riconoscimento facciale di qualsiasi individuo che passa nel raggio di una fotocamera, comprese le persone che non hanno acconsentito al riconoscimento (per es. minori che non possono rilasciare un valido consenso).
Ebbene, poiché la finalità è quella di identificare in modo univoco le persone, è evidente che sia necessario fornire un'alternativa al riconoscimento facciale.

Esempio: un hotel utilizza la videosorveglianza per avvisare automaticamente il gestore dell'hotel dell'arrivo di un VIP nel momento in cui il volto dell'ospite viene riconosciuto.
Da un lato c'è il VIP che ha acconsentito all'uso del riconoscimento facciale; dall'altro, vengono raccolti dati biometrici di tutti gli altri ospiti. Tale trattamento sarebbe illecito se non venissero raccolti i consensi di tutti gli ospiti ai sensi dell'Articolo 9, (2), (a), GDPR.

Esempio: un titolare installa un sistema di videosorveglianza con riconoscimento facciale all'ingresso della sala da concerto che gestisce. Il titolare deve impostare gli ingressi in maniera separata: uno con un sistema biometrico e uno senza (dove invece si scansiona per esempio un biglietto).
Gli ingressi dotati di dispositivi biometrici, devono essere installati e resi accessibili in un modo tale da impedire al sistema di catturare dati biometrici di spettatori non consenzienti.

Pertanto, quando il consenso è richiesto dall'Articolo 9 del GDPR, il titolare non deve condizionare l'accesso ai suoi servizi con l'accettazione obbligatoria del riconoscimento biometrico, ma si deve sempre offrire una soluzione alternativa senza trattamento biometrico – cioè senza restrizioni o costi aggiuntivi per l'interessato.

5.2 Misure consigliate per minimizzare i rischi durante il trattamento dei dati biometrici

In base al principio di minimizzazione dei dati, i titolari devono garantire che i dati estratti da un'immagine digitale sia proporzionata alla finalità perseguita.
La conservazione dei dati deve essere garantita in ambienti altamente sorvegliati ed ad accesso ridotto per impedire l'accesso non autorizzato.
Bisogna garantire

- la sicurezza dei dati immagazzinati (ad esempio utilizzando la crittografia);
- la disponibilità;
- l'integrità; e

- la riservatezza dei dati trattati.

Inoltre potrebbe essere utile procedere alla cancellazione dei dati grezzi (immagini del viso, segnali vocali, o l'andatura, ecc.).

6 I diritti degli interessati

6.1 Diritto di accesso

Oltre alle regole generali fornite dal GDPR, ogni interessato ha il diritto di sapere se il sistema di video sorveglianza tratta dai personali o meno ed in caso affermativo si possono successivamente esercitare i diritti di cui all'Articolo 15 e ss. GDPR con alcune precisazioni.

• L'applicazione pratica dell'Articolo 15, paragrafo 4, del GDPR, può incidere negativamente sui diritti degli altri interessati.

Infatti una video registrazione contiene i dati personali di altri soggetti interessati.
La richiesta di un soggetto di voler ricevere una copia di una registrazione (in applicazione dell'articolo 15 (3) cit.) potrebbe influire negativamente sui diritti e le libertà di altri soggetti interessati dallo stesso materiale.
Per evitare questo effetto collaterale, il titolare potrebbe non divulgare il video per evitare che altri soggetti possano essere identificati. Ciò ovviamente non potrebbe essere usata come scusa laddove non vi sia alcun interesse contrapposto di altri interessati.
A tal fine potrebbero essere utilizzati degli strumenti per coprire i volti delle persone (ad esempio, tramite la modifica delle immagini come *masking* o *scrambling*).

• Articolo 11, paragrafo 2, del GDPR, il titolare non è in grado di identificare l'interessato.

Può capitare che dal filmato non sia semplice ricercare i dati personali richiesti.

Per questi motivi l'interessato dovrebbe specificare nella sua richiesta il periodo di riferimento (ad esempio un termine o un luogo).

Esempio: se un soggetto richiede una copia dei propri dati personali elaborati tramite videosorveglianza all'ingresso di un centro commerciale con 30.000 visitatori al giorno, il soggetto deve specificare quando e dove presumibilmente sarebbe stato ripreso. Se altri soggetti possono essere identificati nello stesso video, allora dovrebbero essere resi anonimi i dati dei terzi (ad esempio sfocando le parti non necessarie all'interessato) prima di consegnare la copia all'interessato.

Se il titolare non è in grado di soddisfare la richiesta dovrà dare notizia all'interessato della ricerca senza successo.

Esempio: se il titolare cancella automaticamente tutte le registrazioni ad esempio entro 2 giorni, tale informazione deve essere comunicata all'interessato.

• Articolo 12 del GDPR, richieste eccessive

In caso di richieste eccessive o manifestamente infondate da parte dell'interessato, il titolare può alternativamente addebitare un compenso ragionevole ai sensi dell'articolo 12, paragrafo 5, lettera a), del GDPR, oppure rifiutare di processare la richiesta (articolo 12, paragrafo 5, lettera b), del GDPR.
L'eccessività della richiesta deve essere motivata e dimostrata.

6.2 Diritto alla cancellazione e diritto di opposizione

6.2.1 Diritto alla cancellazione (diritto all'oblio).

Quando i dati personali non sono più necessari per le finalità per la quale sono stati inizialmente memorizzati, o quando il trattamento è illegale (vedi anche sezione 8), l'interessato può esercitare i diritti di cui all'art. 17 GDPR, quindi chiedere che i dati vengano cancellati, ad esempio, laddove:

- il consenso venga revocato e non vi sia altra base giuridica;
- oppure, anche in caso di legittimo interesse, l'interessato abbia esercitato il diritto di opposizione al trattamento (sezione 6.2.2).

Immaginiamo che il titolare renda pubblico un filmato (ad es. durante una trasmissione o *streaming online*), successivamente a seguito di una richiesta di cancellazione dei dati a mente dell'Articolo 17, paragrafo 2, GDPR deve porre in essere tutte le misure necessarie (anche informando altri titolari) oltre che in conformità dell'Articolo 19 GDPR.

Oltre all'obbligo del titolare di cancellare i dati personali su richiesta dell'interessato, è altresì tenuto a limitare i dati raccolti (cfr. sezione 8).
Per esempio sfocare l'immagine e rendendo irreversibile tale modifica equivale a cancellare i dati perché non è possibile ripristinare i dati precedentemente acquisiti e quindi identificare alcun interessato.

Esempio: un minimarket sta avendo problemi con atti di vandalismo, in particolare all'esterno dei locali; pertanto ha installato un sistema di videosorveglianza all'ingresso, adiacente ai muri perimetrali.
Un passante chiede di cancellare i suoi dati personali.
Il titolare è tenuto a rispondere alla richiesta senza ritardo e non oltre un mese.
Poiché il filmato in questione non soddisfa più le finalità per cui era inizialmente memorizzato (nessun vandalismo si è verificato durante il tempo in cui il passante è stato registrato), non vi è alcun legittimo interesse ad archiviare i dati e quindi il titolare deve cancellare i dati personali del passante.

6.2.2 Diritto di opposizione al trattamento dati.

Laddove la base giuridica della videosorveglianza si basi su un legittimo interesse (articolo 6, paragrafo 1, lettera f), GDPR) o un interesse pubblico (articolo 6, paragrafo 1, lettera e), GDPR), l'interessato ha il diritto, in qualsiasi tempo - di opporsi al trattamento in base all'Articolo 21 del GDPR.
In questo caso deve essere effettuato un bilanciamento di interessi.
Il titolare, senza ritardo o entro un mese, deve motivare le ragioni per cui ritiene prevalenti le basi giuridiche sul diritto dell'interessato ad opporsi al trattamento.
Il diritto di opposizione potrebbe essere manifestato durante la video registrazione (ad esempio all'entrata ovvero dopo aver lasciato l'area monitorata).
Insomma, a meno che il titolare non abbia motivi legittimi per mantenere in atto la video registrazione, egli deve essere in grado di:

1) interrompere immediatamente la video registrazione una volta richiesto; o
2) assicurare che l'area monitorata è così circoscritta da non coinvolgere i dati personali dell'interessato né quest'ultimo ha possibilità di accedervi perché non abilitato a farlo (ad es. accesso esclusivo del personale autorizzato).

Quando si utilizza la videosorveglianza per scopi di *marketing* diretto, l'interessato ha il diritto di opporsi al trattamento a sua discrezionalità in quanto il diritto di opporsi in tale contesto è assoluto (articolo 21, (2) e (3), GDPR).

Esempio: una società sta incontrando difficoltà in merito alle violazioni della sua sicurezza, specie in corrispondenza dell'ingresso pubblico ed utilizza la videosorveglianza per motivi di legittimo interesse, allo scopo di acciuffare quelli che fanno ingresso illegalmente.
Un visitatore si oppone al trattamento dei suoi dati attraverso il sistema di videosorveglianza per motivi relativi alla sua particolare situazione.

La società però in questo caso respinge la richiesta con la spiegazione che la video registrazione è necessaria per finalità di un'indagine interna in corso, quindi al diritto di opposizione sopravvive un legittimo interesse del titolare.

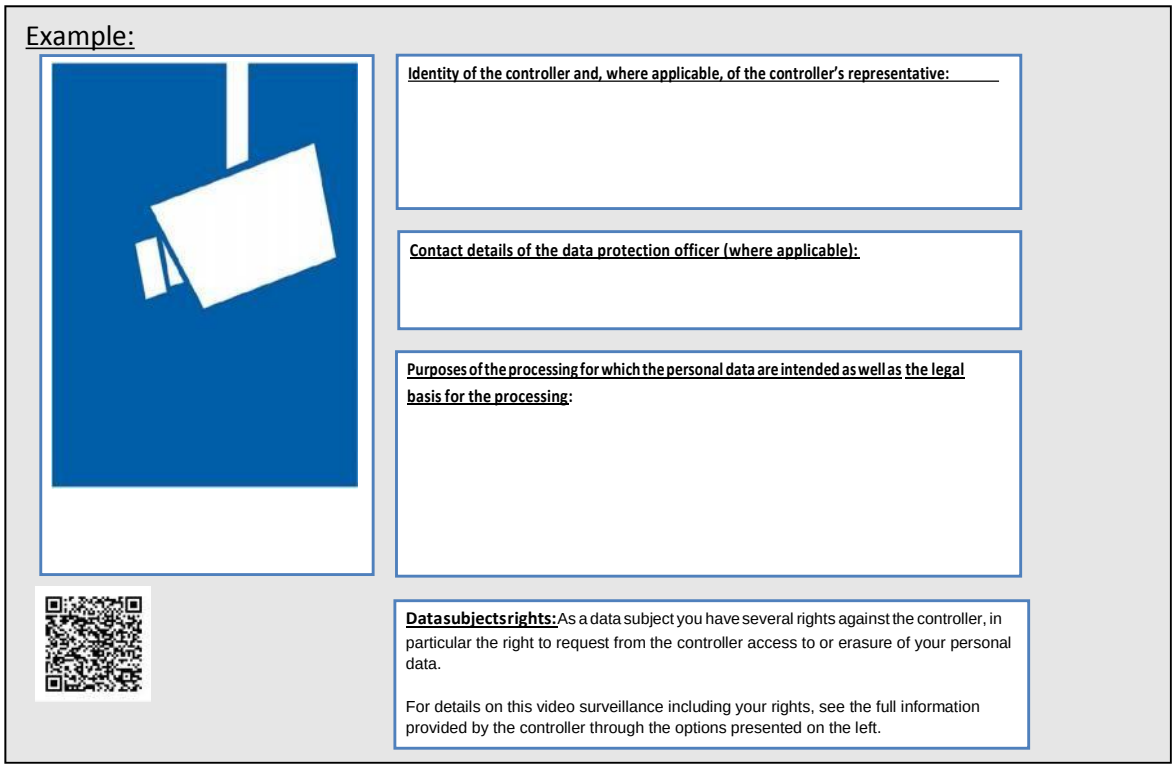
7 Obblighi di trasparenza e informazione

La prima informazione da fornire agli interessati riguarda i luoghi in cui avviene la video sorveglianza.
Vi dovrebbe essere

- un **primo livello** di informazione costituito da un segnale di avvertimento;
- un **secondo livello** di informazione dove vengono fornite informazioni ulteriori.

7.1 Informazioni sul primo livello (segnale di avvertimento)

L'EDPB fornisce un esempio di segnale (vedi la figura sottostante)



In particolare il segnale fornisce in modo facile ed intuitivo, una panoramica significativa del trattamento effettuato (articolo 12, (7), GDPR).

Inoltre tale segnale dovrebbe essere posizionato su ogni singola postazione di video registrazione.

7.1.1 Posizionamento del segnale di avvertimento

Il segnale non dovrebbe essere troppo distante dalla postazione di video registrazione in modo tale che l'interessato possa facilmente riconoscere la finalità della videosorveglianza (approssimativamente ad altezza occhi).
Non è necessario specificare precisamente ove il sistema è collocato ma deve essere chiara l'area video sorvegliata.

7.1.2 Contenuto dell'informazione di primo livello

Le informazioni di primo livello contengono le informazioni più importanti, ad es

- i dettagli delle finalità del trattamento;
- l'identità del titolare;
- l'elencazione dei diritti dell'interessato;
- informazioni sugli impatti del trattamento (ad esempio la base giuridica del trattamento);
- l'indicazione del DPO.

7.2 Informazioni di secondo livello

Anche le informazioni di secondo livello devono essere rese disponibili in un luogo facilmente accessibile agli interessati.
Ad esempio, un foglio informativo completo dovrebbe essere disponibile in una posizione centrale (*reception*) o visualizzabile su un poster facilmente accessibile.
Le informazioni di secondo livello possono già essere richiamate da quelle di primo livello (ad esempio codice QR o indirizzo di un sito Web) oppure disponibili non digitalmente.
In ogni caso, deve essere possibile accedere alle informazioni di secondo livello senza accedere all'area videosorvegliata.
L'informazione di secondo livello deve contenere tutte le altre informazioni obbligatorie ai sensi dell'Articolo 13 del GDPR.
Inoltre, il titolare può fornire informazioni più efficaci e dettagliate.

Esempio: il proprietario di un negozio sta monitorando il suo negozio. Per conformarsi all'Articolo 13 è sufficiente posizionare un segnale di avvertimento in un punto facilmente visibile all'ingresso del suo negozio, che contiene le informazioni di primo livello.
Inoltre, deve fornire un foglio informativo contenente le informazioni di secondo livello al cassiere o posizionarla in qualsiasi altra posizione centrale e facilmente accessibile nel suo negozio.

8 Periodo di archiviazione e obbligo di cancellazione

I dati personali non possono essere archiviati per un tempo eccessivo e non necessario alle finalità i quali vengono raccolti (articolo 5 (1) (c) ed (e) GDPR).
Sul punto è utile osservare che gli stati membri adottano regole specifiche.
Spesso la finalità del trattamento è la protezione della proprietà o la conservazione di una prova documentale.
Tale scopo può essere soddisfatto mantenendo la registrazione per pochi giorni (uno o due giorni, in altri casi anche 72 ore).
Il titolare può giustificare la legittimità della finalità e la necessità di archiviazione per un periodo maggiore ma tale necessità deve essere motivata e le misure di sicurezza di archiviazione devono essere maggiori.

Esempio: un proprietario di un piccolo negozio normalmente vuole evitare atti di vandalismo durante il giorno. Di conseguenza, è sufficiente un periodo di conservazione delle videoregistrazioni di 24 ore. Tuttavia, durante le vacanze o il fine settimana, dove il negozio rimane chiuso, il periodo di conservazione potrebbe essere più lungo tanto da coprire il periodo di chiusura, in caso di danneggiamento potrà essere intrapresa un'azione legale contro colpevole.

9 Misure tecniche e organizzative

Il titolare, ai sensi dell'Articolo 32, paragrafo 1, GDPR, deve garantire un elevato *standard* di misure organizzative e tecniche affinché il trattamento dei dati durante la videosorveglianza sia sicuro.

Tali **misure organizzative e tecniche** devono essere **proporzionali ai rischi per i diritti e le libertà degli interessati**, derivanti da

- distruzione accidentale o illecita;
- perdita;
- alterazione;
- divulgazione non autorizzata;
- accesso ai dati di videosorveglianza non autorizzato.

Ai sensi degli Articoli 24 e 25 del GDPR, i titolari attuano le misure tecniche e organizzative anche al fine di salvaguardare la protezione dei dati e per consentire l'esercizio dei diritti stabiliti agli Articoli 15 - 22 GDPR.
Ciò presume un'implementazione costante e una DPIA preventiva.

9.1 Panoramica del sistema di videosorveglianza

Un sistema di videosorveglianza (il GDPR non fornisce una definizione) o *video surveillance system* (VSS) è costituito da dispositivi analogici e digitali nonché *software* con lo scopo di catturare immagini di una ambiente, gestirne le immagini e visualizzarle tramite operatore.
I suoi componenti sono raggruppabili nelle seguenti categorie:

- **Ambiente video**: acquisizione di immagini, interconnessioni e gestione delle immagini

- La finalità dell'acquisizione delle immagini è la generazione di un'immagine del mondo reale in un formato tale che può essere utilizzato dal resto del sistema;
- le interconnessioni descrivono tutte le trasmissioni di dati all'interno dell'ambiente video (es. connessioni: cavi, reti digitali e trasmissioni wireless; e comunicazioni: descrivono tutti i video e i controlli dei segnali dei dati, che potrebbero essere digitali o analogici);
- la gestione delle immagini include analisi, memorizzazione e presentazione di un'immagine o di una sequenza di immagini.

- Dal punto di vista della gestione del sistema, un VSS ha le seguenti funzioni logiche:

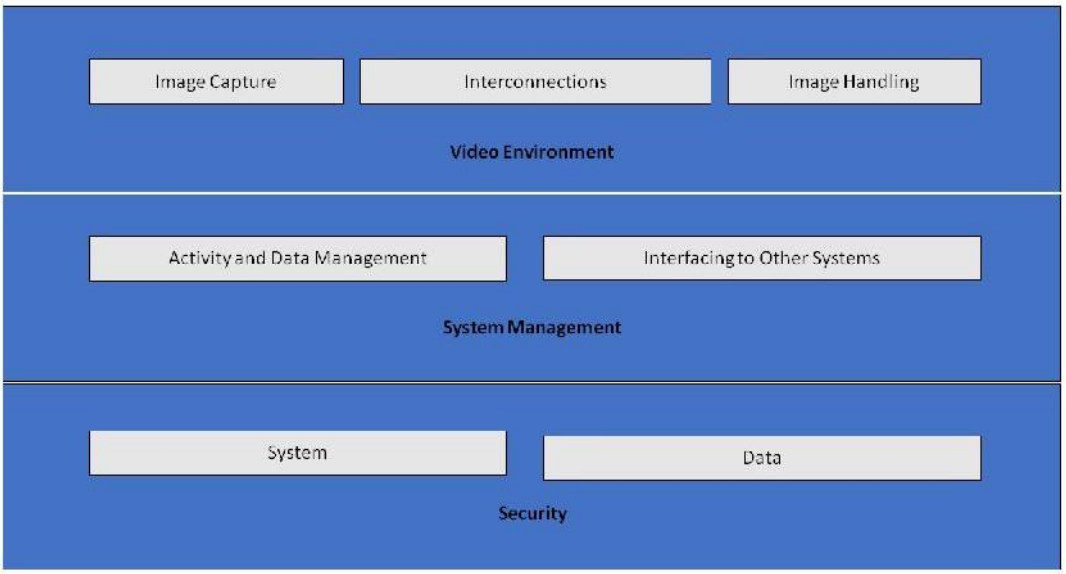
- gestione dei dati e gestione delle attività, che include l'operatore di gestione dei comandi e attività generate dal sistema (procedure di allarme, avvisi degli operatori);
- le interfacce con altri sistemi potrebbero includere la connessione ad altri sistemi di sicurezza (controllo degli accessi, allarme antincendio) e sistemi non di sicurezza (*building management systems*, riconoscimento automatico di targhe)

- La sicurezza VSS comprende riservatezza, integrità e disponibilità dei sistemi e dei dati:

- la sicurezza del sistema include la sicurezza fisica di tutti i componenti del sistema e il controllo di accesso al VSS;

la sicurezza dei dati include la prevenzione della perdita o la manipolazione dei dati.

Sistema di videosorveglianza



9.2 Protezione dei dati by design e by default

Come stabilito nell'Articolo 25 del GDPR, prima che inizi il trattamento dei dati, il titolare deve attuare progettare un'adeguata politica di protezione tecnica ed una gestione organizzativa confacente ad un sistema di videosorveglianza.

Invero, la protezione dei dati si articola su **due livelli**:
- **organizzativo**;
- **tecnico**.

A livello organizzativo, significa stabilire e applicare politiche e procedure relative alla videosorveglianza.
Dal punto di vista tecnico, significa:
- trattare i dati in conformità all'Articolo 5, GDPR (legittimità, finalità e limitazione dei dati, riduzione dei dati);
- trattare i dati ai sensi dell'Articolo 25, paragrafo 2, GDPR (integrità e riservatezza, responsabilità ecc.).
- attuare misure di sicurezza adeguate e pertinenti al dato trattato.

9.3 Esempi concreti di misure adeguate

Indipendentemente dalla soluzione prescelta, il titolare deve proteggere adeguatamente tutti i componenti di un sistema di videosorveglianza in tutte le sue fasi
- dati a riposo;
- dati in transito; e,
- dati in uso.

Per questo è necessario unire l'organizzazione con le misure tecniche prescelte.

Sono da preferire sistemi in grado di proteggere anche la privacy: ad esempio sistemi che consentono il *mascking* o lo *scrambling*; oppure sistemi in linea con gli standard IT a livello internazionale (ISO / IEC 27000 - Serie di sistemi di gestione della sicurezza delle informazioni).

9.3.1 Misure organizzative

A parte la necessità di DPIA (cfr. la sezione 10), il titolare deve predisporre politiche e procedure organizzative specifiche per la videosorveglianza.
In particolare deve stabilire:

- chi è responsabile della gestione e del funzionamento del sistema di videosorveglianza;
- finalità e ambito del progetto di videosorveglianza;
- l'uso lecito e illecito della video sorveglianza (dove e quando è consentita la videosorveglianza e dove e quando non lo è; ad esempio uso di telecamere nascoste e audio oltre alla registrazione video)
- in maniera adeguate le informazioni da divulgare di cui alla sezione 7 (Trasparenza e obblighi di informazione);
- come vengono registrati i video e per quale durata, inclusa l'archiviazione dei filmati e messa in sicurezza in caso di incidenti;
- chi deve essere sottoposto alla formazione specifica e nelle tempistiche previste;
- chi ha accesso alle registrazioni video e per quali finalità;
- procedure operative (ad es. da chi e da dove viene monitorata la videosorveglianza, che cosa fare in caso di un *data breach*);
- quali procedure devono seguire i soggetti esterni per richiedere registrazioni video e procedure per negare o assecondare tali istanze;
- procedure per l'acquisizione, l'installazione e la manutenzione di VSS;
- procedure di gestione degli incidenti e di recupero dati.

L'uso di tali tecnologie può essere addirittura obbligatorio (Articolo 5, (1), (c), GDPR).

9.3.2 Misure tecniche

Sicurezza del sistema significa:

- **sicurezza fisica** di tutti i componenti del sistema;
- **integrità del sistema**; ovvero,
- **protezione contro e resilienza in caso di interferenze intenzionali e non intenzionali rispetto alle sue normali operazioni**; e,
- **controllo degli accessi**.

Sicurezza dei dati significa:

- **riservatezza** (i dati sono accessibili solo a determinati soggetti);
- **integrità** (prevenzione contro la perdita o manipolazione dei dati); e,
- **disponibilità** (i dati possono trattati laddove sia richiesto).

La sicurezza fisica significa proteggere fisicamente l'infrastruttura VSS da furto, atti vandalici, calamità naturali, catastrofi dovute all'uomo e danni accidentali (ad es. da picchi elettrici, temperature estreme e caffè).

Sicurezza dei sistemi e dei dati, ovvero protezione contro interferenze intenzionali e involontarie rispetto alle normali operazioni possono includere:

- protezione dell'intera infrastruttura VSS (comprese telecamere remote, cablaggio e alimentazione) contro manomissioni e furti fisici;
- protezione della trasmissione di filmati con canali di comunicazione sicuri contro l'intercettazione;
- crittografia dei dati;
- utilizzo di soluzioni *hardware* e *software* come *firewall*, antivirus o sistemi di rilevamento intrusioni contro gli attacchi informatici;

- rilevamento di guasti di componenti, *software* e interconnessioni;
- ripristino della disponibilità di accesso al sistema in caso di problemi fisici o tecnici dovuti a incidente.

Il controllo dell'accesso garantisce che solo le persone autorizzate possano accedere al sistema e ai dati.

Le misure di controllo fisico e logico includono:
- garantire che tutti i locali in cui il monitoraggio della videosorveglianza o i filmati vengano archiviati siano protetti da accessi non autorizzati di terzi;
- posizionare i monitor in modo che solo gli operatori autorizzati possano vederli;
- definire in maniera specifica e rigorosa le procedure di concessione, modifica e revoca degli accessi fisici e logici;
- implementare i metodi e mezzi per l'autenticazione e l'autorizzazione dell'utente, compresa la durata e la modifica delle password;
- rivedere periodicamente le azioni eseguite dall'utente e loro registrazione;
- monitorare ed individuare i guasti di accesso in modo continuativo ed individuare le relative carenze il prima possibile.

10 DPIA

Ai sensi dell'Articolo 35, paragrafo 1, GDPR, il titolare è tenuto ad effettuare una DPIA quando un determinato trattamento può comportare un rischio elevato per i diritti e le libertà delle persone fisiche.
Ciò avviene, appunto, nel caso di un monitoraggio sistematico di area pubblicamente accessibili e con il trattamento dei dati su larga scala.
Inoltre, a norma dell'articolo 35, paragrafo 3, lettera b), GDPR, la DPIA è necessaria quanto si trattano dati particolari su larga scala.
Sul punto, le linee guida sulla DPIA forniscono indicazioni maggiori valutazione.
Inoltre, a mente dell'Articolo 35, paragrafo 4, GDPR, l'Autorità Garante nell'ALLEGATO 1 AL PROVVEDIMENTO N. 467 DELL'11 OTTOBRE 2018 [doc. web n. 9058979] (Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018) ha stilato l'elenco dei trattamenti che abbisognano di DPIA obbligatoria.
È ragionevole presumere che molti dei casi di videosorveglianza richiedono una DPIA ed i titolari dovrebbero implementare le misure di protezione dei dati.
Nel caso in cui la DPIA dovesse indicare alti rischi nonostante le misure di sicurezza pianificate dal titolare, a quel punto sarà necessario consultare preventivamente - ai sensi dell'Articolo 36, GDPR- l'Autorità Garante.

GDPR: Linee guida per la videosorveglianza.
Di Valentino Vescio di Martirano.