Linee Guida 3/2019 sul trattamento di dati personali attraverso Videosorveglianza

(Adottato dall'EDPB in assemblea plenaria il 10 Luglio 2019)

(Release 1.1)

Traduzione a cura del Collegio Italiano Privacy

Gradite eventuali segnalazioni o suggerimenti a info@collegioprivacy.it

Indice

Sommario

Il Comitato Europeo per la Protezione dei Dati

Visto l'articolo 70, paragrafo 1 sexies, del Regolamento 2016/679 / UE del Parlamento europeo e del Consiglio del 27 aprile 2016 sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali dati e sulla libera circolazione di tali dati e che abroga la direttiva 95/46 / CE (di seguito "GDPR"),

visto l'accordo SEE e in particolare l'allegato XI e il protocollo 37, come modificato con decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018,

visto l'articolo 12 e l'articolo 22 del suo regolamento interno del 25 maggio 2018, riveduto il 23 Novembre 2018,

HA ADOTTATO LE SEGUENTI LINEE GUIDA

1. INTRODUZIONE.

1. L'uso intensivo di dispositivi video ha un impatto sul comportamento dei cittadini. L'implementazione significativa di strumenti digitali in molte sfere della vita degli individui eserciterà un'ulteriore pressione sull'individuo e bisogna impedire la rilevazione di ciò che potrebbe essere percepito come un'anomalia. Di fatto, queste tecnologie possono restringere le possibilità di movimento anonimo e l'utilizzo anonimo dei servizi, e in genere limitare la possibilità di rimanere inosservati. Le implicazioni sulla protezione dei dati sono enormi.

2. Mentre gli individui potrebbero sentirsi a proprio agio con la videosorveglianza impostata per una determinata finalità (di sicurezza, ad esempio), devono essere prese garanzie per evitare qualsiasi uso improprio di tali dati e l'utilizzo con finalità eccedenti (ad es. finalità di marketing, monitoraggio delle prestazioni dei dipendenti, ecc.). Inoltre, ora molti strumenti sono implementati per sfruttare le immagini catturate trasformando le telecamere tradizionali in telecamere intelligenti. La quantità di dati generati dal video, combinati con questi strumenti tecnologici aumentano i rischi di un uso secondario (correlati o non correlati alla finalità originariamente assegnata al sistema) o anche i rischi di uso improprio. Quando si tratta la videosorveglianza dovrebbero essere sempre considerati con attenzione i principi generali del GDPR (art.5)

3. I sistemi di videosorveglianza cambiano il modo in cui i professionisti del privato e del settore pubblico interagiscono in luoghi privati o pubblici allo scopo di migliorare la sicurezza, realizzando analisi del pubblico, fornendo pubblicità personalizzata, ecc. . La videosorveglianza è diventata altamente performante attraverso la crescente implementazione di analisi intelligenti dei video. Queste tecniche possono essere più invadenti (ad es. tecnologie biometriche complesse) o meno intrusive (ad es. semplici algoritmi di conteggio). In generale è sempre più difficile restare anonimi e preservare la propria privacy. I problemi di protezione dei dati emersi in varie situazioni possono essere svariati, così come lo sarà l'analisi legale quando si utilizza una o l'altra di queste tecnologie.

4. Oltre ai problemi di privacy, ci sono anche rischi legati a possibili malfunzionamenti di questi dispositivi e ai pregiudizi che ne possono derivare. I ricercatori riferiscono che il software utilizzato per il riconoscimento o l'analisi del viso si comporta diversamente in base all'età, al sesso e all'etnia della persona che sta identificando. Gli algoritmi si comporterebbero in base a dati demografici diversi, e pertanto la propensione al riconoscimento facciale rischia di rafforzare i pregiudizi della società. Questo è il motivo per cui i Titolari del trattamento devono anche garantire che il trattamento biometrico dei dati

rilevati dalla videosorveglianza sia soggetto a una valutazione regolare della sua pertinenza e devono fornire sufficienti garanzie.

5. La videosorveglianza non è di default una necessità quando esistono altri mezzi per raggiungere la medesima finalità. Altrimenti rischiamo un cambiamento nelle norme culturali che porta come principio generale all'accettazione della mancanza di privacy.

6. Le presenti linee guida mirano a fornire indicazioni su come applicare il GDPR in relazione al trattamento personale dati tramite dispositivi video. Gli esempi non sono esaustivi, ma sarà possibile applicare i criteri generali in tutte le potenziali aree di utilizzo.

2. AMBITO DI APPLICAZIONE[1].

2.1 Dati Personali

7. Il monitoraggio automatico sistematico di uno spazio specifico tramite mezzi ottici o audiovisivi, principalmente per finalità di protezione della proprietà o della vita e della salute dell'individuo, è diventato un significativo fenomeno dei nostri giorni. Questa attività comporta la raccolta e la conservazione di immagini o audiovisivi su tutte le persone che entrano nello spazio monitorato con la loro identificazione in base al loro aspetto o ad altri elementi specifici. L'identità di queste persone può essere individuata sulla base di questi dettagli. Tale monitoraggio consente inoltre ulteriori trattamenti dei dati personali per quanto riguarda la presenza e il comportamento delle persone in uno spazio determinato. Il potenziale rischio di uso improprio di questi dati aumenta in relazione alla dimensione dello spazio monitorato, nonché al numero di persone che frequentano tale spazio. Questo situazione è contemplata dal Regolamento Generale sulla protezione dei dati di cui all'articolo 35, paragrafo 3, lettera c), che prevede come misura di protezione dei dati la valutazione d'impatto in caso di monitoraggio sistematico di un'area accessibile al pubblico su larga scala, come anche all'articolo 37, paragrafo 1, lettera b), che impone ai Titolari del trattamento di designare un Titolare della Protezione dei Dati se il trattamento per sua natura comporta un monitoraggio regolare e sistematico degli interessati.

8. Tuttavia, il regolamento non si applica al trattamento di dati che non hanno alcun riferimento a una persona, ad esempio nel caso di individuo che non può essere direttamente o indirettamente identificato,.

9.

Esempio: Il GDPR non è applicabile per le fotocamere false (ovvero qualsiasi fotocamera che non funziona come fotocamera e quindi non tratta alcun dato personale). *Tuttavia, in alcuni Stati membri il caso potrebbe essere soggetto normative locali.*

Esempio: Le registrazioni effettuate da un'altezza elevata rientrano nell'ambito di applicazione del GDPR solo se i dati trattati possono essere correlati a una persona specifica.

Esempio: Una videocamera è integrata in un'automobile per fornire assistenza al parcheggio. Il GDPR non si applica se la fotocamera è costruita o regolato in modo tale da non raccogliere alcuna informazione relativa a persone fisiche (come targhe o informazioni che potrebbero identificare i passanti).

[1] L'EDPB osserva che laddove il GDPR lo consenta, potrebbero essere previsti requisiti specifici nella legislazione nazionale.

2.2 Applicazione della Direttiva EU2016/680.

10. In particolare rientra nel campo di applicazione della direttiva EU2016/680 il trattamento di dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, compresa la protezione e la prevenzione delle minacce alla pubblica sicurezza,.

2.3 Esenzione nella sfera privata.

11. Ai sensi dell'articolo 2, paragrafo 2, lettera c), non rientra nell'ambito di applicazione del GDPR[2] il trattamento di dati personali da parte di una persona fisica nel corso di un'attività puramente personale o domestica, che può anche includere attività online.

12. Questa disposizione - la cosiddetta esenzione domestica - nel contesto della videosorveglianza deve essere interpretata in modo restrittivo. Pertanto, come considerato dalla Corte di Giustizia Europea, la cosiddetta "esenzione familiare" deve essere "*interpretata come relativa alle sole attività svolte nel corso della vita privata o familiare delle persone, che chiaramente non è il caso del trattamento di dati personali derivanti dalla pubblicazione su Internet, che comporta che tali dati siano resi accessibili a un numero indefinito di persone*"[3]. Inoltre, se un sistema di videosorveglianza, nella misura in cui comporta la registrazione e l'archiviazione costanti di dati personali inquadrando, "*anche parzialmente, uno spazio pubblico e di conseguenza diretta verso l'esterno da una installazione privata, non può essere considerata un'attività puramente 'personale o domestica' ai fini dell'articolo 3, paragrafo 2, secondo comma della Direttiva Europea 1995/46*"[4].

13. Per quanto riguarda i dispositivi video gestiti all'interno dei locali di un privato, il caso potrebbe rientrare nell'esenzione da parte delle famiglie. Dipenderà da diversi fattori, che dovranno tutti essere valutati per giungere una conclusione. Oltre agli elementi sopra menzionati identificati dalle sentenze della Corte di Giustizia Europea, l'utente della videosorveglianza privata deve verificare se ha qualche tipo di relazione personale con l'interessato, se la scala o la frequenza della sorveglianza suggerisce un tipo di attività professionale dell'interessato e del potenziale impatto negativo della sorveglianza sugli stessi interessati. La presenza di uno solo dei suddetti elementi non suggerisce necessariamente che il trattamento non rientra nell'ambito dell'esenzione per le famiglie: è necessaria una valutazione globale.

[2] Vedi anche il considerando 18.

[3] Corte di giustizia europea, sentenza relativa alla causa C-101/01, *caso Bodil Lindqvist*, 6 novembre 2003, punto 47.

[4] Corte di giustizia europea, sentenza relativa alla causa C-212/13, *František Ryneš contro Úřad pro ochranu osobních údajů*, 11 dicembre 2014, par. 33.

14.

Esempio: Un turista sta registrando un video tramite un telefono cellulare o una videocamera per documentare le sue vacanze. Mostra il filmato ad amici e parenti ma non lo rende accessibile a un numero indefinito di persone. Questo caso rientrerebbe nell'esenzione domestica.

Esempio: Un mountainbiker in escursione vuole registrare la sua discesa con una actioncam. Sta operando in una zona remota e prevede di utilizzare le registrazioni solo per il suo intrattenimento personale a casa. Questo caso rientrerebbe nell'esenzione domestica.

Esempio: Un soggetto sta monitorando e registrando il proprio giardino. La proprietà è recintata ed entrano regolarmente nel giardino solo lo stesso proprietario e la sua famiglia. Ciò rientrerebbe nell'esenzione domestica, a condizione che la videosorveglianza non si estenda neanche parzialmente a uno spazio pubblico o a una proprietà vicina.

3. LEGITTIMITA' DEL TRATTAMENTO.

15. Prima dell'uso, devono essere specificate in dettaglio le finalità del trattamento (articolo 5, paragrafo 1, lettera b)). La videosorveglianza può raggiungere varie finalità, ad esempio la protezione della proprietà e di altri beni, o la raccolta di prove per azioni civili[5]. Queste finalità di monitoraggio devono essere documentate per iscritto (articolo 5, paragrafo 2) e devono essere specificate per ogni telecamera di sorveglianza in uso. Le telecamere utilizzate da un singolo Titolare per la medesima finalità possono essere documentate insieme, purché ogni telecamera utilizzata indichi le specifiche finalità. Inoltre, gli interessati devono essere informati sulle finalità del trattamento in conformità all'articolo 13 (*vedere sezione 7, Trasparenza e obblighi di informazione*). La videosorveglianza basata sulla mera finalità di "sicurezza" o "per la propria sicurezza" non è sufficientemente specifica (articolo 5, paragrafo 1, lettera b)). È inoltre contraria al principio secondo cui i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (cfr. L'articolo 5, paragrafo 1, lettera a)).

16. In linea di principio, ogni motivazione legale ai sensi dell'articolo 6, paragrafo 1, può fornire una base giuridica per il trattamento dei dati di videosorveglianza. Ad esempio, laddove la legislazione nazionale preveda un obbligo di videosorveglianza[6] si applica l'articolo 6, paragrafo 1, lettera c). Tuttavia, nella pratica, le disposizioni che possono essere utilizzate sono:

- Articolo 6, paragrafo 1, lettera f) (legittimo interesse).

- Articolo 6, paragrafo 1, lettera e) (necessità di svolgere un compito nell'interesse pubblico o nell'esercizio di una pubblica autorità)

In casi eccezionali, come base giuridica potrebbe essere utilizzato dal Titolare del trattamento l'articolo 6, paragrafo 1, lettera a) (consenso)**.**

[5] Le regole sulla raccolta delle prove per le cause civili variano nei singoli Stati membri.
[6] Queste linee guida non analizzano o entrano nei dettagli delle legislazioni nazionali che potrebbero differire tra gli Stati membri.

3.1 Legittimo interesse (Art. 6 paragrafo 1 comma f)).

17. La valutazione giuridica dell'articolo 6, paragrafo 1, lettera f), deve essere basata su criteri di conformità con il Considerando 47.

3.1.1 Esistenza di legittimi interessi.

18. La videosorveglianza è lecita se è necessaria per soddisfare la finalità di un interesse legittimo perseguito da un Titolare del trattamento o da un terzo, a meno che tali interessi ignorino gli interessi della persona interessata o i diritti e le libertà fondamentali (articolo 6, paragrafo 1, lettera f)). Gli interessi legittimi perseguiti da un Titolare del trattamento o da un terzo possono essere legali[7], interessi economici o non materiali[8]. Tuttavia, il Titolare del trattamento dovrebbe considerare che se l'interessato si oppone alla sorveglianza ai sensi dell'articolo 21, il Titolare del trattamento può procedere con la videosorveglianza dell'interessato solo qualora abbia un interesse legittimo valido che prevalga sugli interessi, i diritti e le libertà dell'interessato o per esercitare la difesa in azioni giudiziarie.

19. Data una situazione reale e pericolosa, la finalità di proteggere la proprietà da furto con scasso, furto o vandalismo può costituire un interesse legittimo per la videosorveglianza.

20. L'interesse legittimo deve avere reale consistenza e deve essere un problema reale (cioè non deve essere immaginario o speculativo)[9]. Prima di avviare la sorveglianza, è necessario che si verifichi una situazione di disagio nella vita reale, ad esempio danni o incidenti gravi in passato. Alla luce del principio di Responsabilità, i Titolari del trattamento dovrebbero documentare gli incidenti rilevanti (data, modalità, perdita finanziaria) e relative accuse penali. Questi incidenti documentati possono rilevare un adeguato interesse legittimo.

21.

> Esempio: un proprietario desidera aprire un nuovo negozio e installare un sistema di videosorveglianza. Egli può indicare, presentando statistiche, che c'è un'alta aspettativa di vandalismo nel vicinato. Inoltre, è utile l'esperienza dei negozi vicini. Non è necessario che si sia verificato un danno al proprietario in questione. Tuttavia, non è sufficiente presentare statistiche nazionali o generali sulla criminalità senza analizzare l'area in questione o i pericoli per questo negozio specifico.

22. Situazioni di pericolo imminente possono costituire un interesse legittimo, come negozi che vendono beni preziosi (ad esempio gioiellieri) o aree che sono note per essere scene tipiche del crimine per reati di proprietà (ad esempio stazioni di servizio).

23. Inoltre il GDPR afferma chiaramente che per i loro trattamento le autorità pubbliche non devono indicare le motivazioni di legittimo interesse, fintanto che operano nello svolgimento dei loro compiti istituzionali (articolo 6, paragrafo 1, comma 2).

3.1.2 Necessità del Trattamento.

[7] Corte di giustizia europea, sentenza nella causa C-13/16, *causa Rīgas satiksme*, 4 maggio 2017.

[8] vedi wp 217, Gruppo di lavoro Articolo 29.

[9] vedi wp 217, Gruppo di lavoro Articolo 29, pagine 24 e seguenti.

24. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali sono trattati ("minimizzazione dei dati"), cfr. l'articolo 5, paragrafo 1, lettera c). Prima di installare un sistema di videosorveglianza, il Titolare dovrebbe sempre esaminare criticamente se questa misura è in primo luogo adatta per raggiungere l'obiettivo desiderato, e in secondo luogo se è adeguata e necessaria per le relative finalità. Le misure di videosorveglianza dovrebbero essere scelte solo se le finalità del trattamento non possano ragionevolmente essere raggiunte con altri mezzi meno invasivi dei diritti e delle libertà fondamentali dell'interessato.

25. Data la situazione in cui un Titolare vuole prevenire reati connessi alla proprietà, invece di installare un sistema di videosorveglianza, il Titolare potrebbe anche adottare misure di sicurezza alternative come recintare la proprietà, installare pattuglie regolari del personale di sicurezza, utilizzare i portieri/custodi, fornire una migliore illuminazione, installare la sicurezza serrature, finestre e porte a prova di manomissione o applicazione di rivestimento antigraffiti o lamine alle pareti. Tali misure possono essere efficaci quanto i sistemi di videosorveglianza contro furto con scasso, furto e atti vandalici.

26. Prima di utilizzare un sistema di telecamere, il Titolare è tenuto a valutare dove e quando le misure di videosorveglianza sono strettamente necessarie. Di solito un sistema di sorveglianza che funziona di notte e al di fuori del normale orario di lavoro soddisferà le esigenze del Titolare del trattamento per prevenire pericoli per la sua proprietà.

27. In generale, la necessità di utilizzare la videosorveglianza per proteggere i locali del Titolare finisce ai confini della proprietà[10]. Tuttavia, per una protezione efficace, in alcuni casi potrebbe essere necessario estendere la videosorveglianza nelle immediate vicinanze dei locali. In questo contesto, il Titolare dovrebbe prendere in considerazione mezzi fisici e tecnici, come ad esempio bloccare o pixelare aree non rilevanti.

28.

Esempio: una libreria vuole proteggere i suoi locali da atti vandalici. In generale, le telecamere dovrebbero filmare solo i locali stessi perché per questa finalità non è necessario inquadrare i locali attigui o le aree pubbliche circostanti i locali della libreria.

29. Domande relative alla necessità del trattamento sorgono anche riguardo al modo in cui vengono conservate le registrazioni. In alcuni casi potrebbe essere necessario utilizzare soluzioni di scatola nera in cui il filmato viene automaticamente eliminato dopo un certo periodo di conservazione e vi si accede solo in caso di incidente. In altre situazioni potrebbe non essere necessario registrare il materiale video, ma sarebbe invece più appropriato utilizzare il monitoraggio in tempo reale. La scelta tra le soluzioni della scatola nera e il monitoraggio in tempo reale dovrebbe basarsi anche sulle finalità perseguite. Se ad esempio la finalità della videosorveglianza è la conservazione delle prove, i metodi in tempo reale di solito non sono idonei. A volte il monitoraggio in tempo reale può anche essere più invadente della memorizzazione e dell'eliminazione automatica del materiale dopo un periodo di tempo limitato. Il principio di minimizzazione dei dati deve essere considerato in questo contesto (articolo 5, paragrafo 1, comma c)). Va inoltre tenuto presente che potrebbe essere possibile che il Titolare del trattamento possa utilizzare in sostituzione della videosorveglianza il personale di sicurezza che è in grado di reagire e intervenire immediatamente.

3.1.3 Bilanciamento degli interessi.

30. Presumendo che la videosorveglianza sia necessaria per proteggere gli interessi legittimi di un Titolare del trattamento, essa può essere messa in funzione solo se gli interessi legittimi del Titolare o quelli di

[10] Questo in alcuni Stati membri potrebbe anche essere soggetto alle legislazioni nazionali.

terzi (ad es. Protezione della proprietà o integrità fisica) non ledano totalmente gli interessi o i diritti e libertà fondamentali dell'interessato. Il Titolare del trattamento deve considerare:

1) in che misura il monitoraggio influisce sugli interessi legittimi, sui diritti fondamentali e sulle libertà delle persone e

2) se ciò causa violazioni o conseguenze negative in relazione ai diritti dell'interessato.

In effetti, il bilanciamento degli interessi è obbligatorio. Devono essere valutati ed equilibrati attentamente da un lato i diritti e le libertà fondamentali e dall'altro gli interessi legittimi del Titolare del trattamento.

31.

Esempio: Una società di un parcheggio privato ha documentato problemi ricorrenti con furti nelle auto parcheggiate. L'area di parcheggio è uno spazio aperto e può essere facilmente accessibile a chiunque, ma è chiaramente contrassegnato da cartelli e barriere stradali che circondano lo spazio. La società di parcheggio ha un interesse legittimo (prevenire i furti nelle auto del cliente) per monitorare l'area durante le ore diurne in cui si verificano problemi. Gli interessati sono monitorati in un arco di tempo limitato, non si trovano nell'area per scopi ricreativi ed è anche nel loro stesso interesse prevenire i furti. in questo caso è prevalso l'interesse legittimo del Titolare del trattamento sull'interesse dei soggetti interessati a non essere monitorati.

Esempio: Un ristorante decide di installare videocamere nei servizi igienici per controllare l'ordine delle strutture sanitarie. In questo caso i diritti degli interessati prevalgono chiaramente sull'interesse del Titolare del trattamento: pertanto non è possibile installare telecamere in quel luogo.

3.1.3.1 Prendere decisioni caso per caso.

32. Poiché ai sensi del Regolamento il bilanciamento degli interessi è obbligatorio, la decisione deve essere presa caso per caso (cfr. L'articolo 6, paragrafo 1, lettera f)). Non è sufficiente fare riferimento a situazioni astratte o confrontare casi simili tra di loro. Il Titolare del trattamento deve valutare i rischi sulla protezione dei diritti dell'interessato; il criterio decisivo è valutare quanto l'intensità dell'intervento possa ledere i diritti e le libertà dell'individuo.

33. L'intensità dell'intervento può essere definita, tra l'altro, dal tipo di informazioni raccolte (contenuto delle informazioni), dalla portata (densità delle informazioni, estensione spaziale e geografica), dal numero di interessati in questione, come quantità specifica o come una proporzione della popolazione pertinente, dalla situazione in questione, dagli interessi reali degli interessati, dai mezzi alternativi, nonché dalla natura e dalla finalità della valutazione dei dati raccolti.

34. Importanti fattori di bilanciamento possono essere la dimensione dell'area che è sotto sorveglianza e la quantità di persone soggette a sorveglianza. L'uso della videosorveglianza in un'area remota (ad es. Per osservare la fauna selvatica o proteggere infrastrutture critiche come un'antenna radio di proprietà privata) deve essere valutato in modo differente rispetto alla videosorveglianza in una zona pedonale o in un centro commerciale.

Esempio: Se è installata una dash cam (ad es. allo scopo di raccogliere prove in caso di incidente), è importante assicurarsi che questa telecamera non stia registrando costantemente il traffico, così come le persone che si trovano nei pressi della strada. Altrimenti l'interesse ad avere registrazioni video come

prova nel caso più teorico di un incidente stradale non può giustificare questa grave interferenza con i diritti dell'interessato[11].

3.1.3.2 Ragionevoli aspettative degli interessati.

35. Secondo il Considerando 47, l'esistenza di un interesse legittimo richiede un'attenta valutazione. Qui devono essere incluse le ragionevoli aspettative dell'interessato al momento e nel contesto del trattamento dei suoi dati personali. Per quanto riguarda il monitoraggio sistematico, la relazione tra l'interessato e il Titolare del trattamento può variare in modo significativo e può influire sulle aspettative ragionevoli che l'interessato potrebbe avere. L'interpretazione del concetto di aspettative ragionevoli non dovrebbe basarsi solo sulle aspettative soggettive in questione. Piuttosto, il criterio decisivo deve essere valutare se potrebbe ragionevolmente esistere una finalità ulteriore nell'essere soggetto a monitoraggio nella situazione specifica.

36. Ad esempio, nella maggior parte dei casi un dipendente nel suo posto di lavoro probabilmente non si aspetta di essere monitorato dal suo datore di lavoro[12]. Inoltre, non si prevede il monitoraggio in un giardino privato, nelle aree di vita o nelle sale dove si svolgono esami o trattamenti. Allo stesso modo, non è ragionevole aspettarsi un monitoraggio in strutture sanitarie o in una sauna - il monitoraggio di tali aree è una notevole intrusione nei diritti dell'interessato. Le ragionevoli aspettative degli interessati sono che nessuna sorveglianza video avrà luogo in quelle aree. D'altro canto, il cliente di una banca potrebbe aspettarsi di essere monitorato all'interno della banca medesima o davanti al bancomat.

37. Le persone interessate possono anche aspettarsi di non essere monitorate all'interno di aree pubbliche, in particolare se tali aree pubbliche sono in genere utilizzate per attività di recupero, rigenerazione e svago, nonché nei luoghi in cui le persone soggiornano e/o comunicano, come aree salotto, tavoli nei ristoranti, parchi, cinema e strutture per il fitness. Qui gli interessi legittimi o i diritti e le libertà dell'interessato devono prevalere in linea di principio sugli interessi legittimi del Titolare del trattamento.

37.

Esempio: Nei servizi igienici gli interessati si aspettano di non essere monitorati. In questo caso la videosorveglianza per prevenire incidenti non è proporzionale.

39. I cartelli che informano l'interessato in merito alla videosorveglianza non hanno rilevanza nel determinare ciò che l'interessato può obiettivamente aspettarsi.

3.2 Necessità di svolgere un compito eseguito di pubblico interesse o nell'esercizio di un'Autorità Ufficiale nel ruolo di Titolare del trattamento, articolo 6, paragrafo 1, lettera e).

40. Potrebbero essere trattati dati personali mediante videosorveglianza ai sensi dell'articolo 6, paragrafo 1, lettera e), se è necessario svolgere un compito eseguito nell'interesse pubblico o nell'esercizio di

[11] Anche se in alcune circostanze potrebbe teoricamente essere possibile identificare una base giuridica per parti di tale sorveglianza, il Titolare del trattamento dovrà comunque rispettare i principi generali (art. 5 GDPR) e gli obblighi di trasparenza per informare correttamente l'interessato (art. 13 GDPR).

[12] Vedi anche: Gruppo di lavoro Articolo 29, parere 2/2017 sul trattamento dei dati sul lavoro WP249, adottato l'8 giugno 2017.

un'Autorità Ufficiale[13]. È possibile che l'esercizio di un'Autorità Ufficiale non consenta tale trattamento, ma altre basi legislative come "salute e sicurezza" per la protezione di dipendenti, visitatori e dipendenti possono prevedere un campo di applicazione limitato per il trattamento, pur tenendo conto degli obblighi del GDPR e dei diritti dell'interessato.

41. Gli Stati membri possono mantenere o introdurre una legislazione nazionale specifica per la video-sorveglianza adattando l'applicazione delle norme del GDPR e determinando requisiti più precisi specifici per il trattamento, purché sia conforme ai principi stabiliti dal GDPR (ad esempio limitazione della conservazione, proporzionalità).

3.3 Consenso, Articolo 6 paragrafo 1 lettera a).

42. Il consenso deve essere dato liberamente, e deve essere specifico, informato e inequivocabile come descritto nelle linee guida sul consenso.[14]

43. Per quanto riguarda il monitoraggio sistematico, il consenso dell'interessato può servire come base giuridica ai sensi dell'articolo 7 (cfr. Considerando 43) solo in casi eccezionali. È nella natura della videosorveglianza che questa tecnologia monitora contemporaneamente un numero indefinito di persone. Il Titolare del trattamento difficilmente sarà in grado di dimostrare che l'interessato ha dato il proprio consenso prima del trattamento dei propri dati personali (articolo 7, paragrafo 1). Supponendo che l'interessato ritiri il proprio consenso, sarà difficile per il Titolare del trattamento dimostrare che i dati personali non vengono più trattati (articolo 7, paragrafo 3).

44.

> Esempio: Gli atleti possono richiedere il monitoraggio durante i singoli esercizi per analizzare le loro tecniche e prestazioni. D'altra parte, quando una società sportiva prende l'iniziativa di monitorare un'intera squadra per la stessa finalità, il consenso spesso non sarà valido, poiché i singoli atleti potrebbero sentirsi spinti a dare il consenso per evitare che il loro rifiuto del consenso influisca negativamente sui compagni di squadra.

45. Se il Titolare del trattamento desidera fare affidamento sul consenso, è suo dovere assicurarsi che ogni persona interessata che accede all'area sottoposta a videosorveglianza abbia dato il proprio consenso. Questo consenso deve soddisfare le condizioni di cui all'articolo 7. Entrare in un'area monitorata contrassegnata (ad esempio, le persone sono invitate ad attraversare un corridoio o cancello specifico per entrare in un'area monitorata), non costituisce una dichiarazione o una chiara azione affermativa necessaria per il consenso, a meno che non soddisfi i criteri di cui agli articoli 4 e 7 come descritto negli orientamenti sul consenso.[15]

46. Dato lo squilibrio di potere tra datori di lavoro e dipendenti, nella maggior parte dei casi i datori di lavoro non dovrebbero fare affidamento sul consenso durante il trattamento dei dati personali, poiché è improbabile che venga fornito liberamente. In questo contesto dovrebbero essere prese in considerazione le linee guida sul consenso.

---

[13] La base per il trattamento cui si fa riferimento «è stabilita dal diritto dell'Unione o dal diritto degli Stati membri» ed «è necessaria per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio dell'autorità ufficiale investita del Titolare del trattamento» (articolo 6 comma 3)).

[14] Inoltre, il Gruppo di lavoro Articolo 29 ha adottato "Linee guida sul consenso ai sensi del Regolamento Europeo 2016/679" (WP 259 rev. 01) che dovrebbero essere prese in considerazione.

[15] Inoltre, il Gruppo di lavoro Articolo 29 ha adottato "Linee guida sul consenso ai sensi del Regolamento Europeo 2016/679" (WP 259) che dovrebbero essere prese in considerazione.

47. Le leggi o gli accordi collettivi degli Stati membri, inclusi gli "accordi di lavoro aziendali", possono prevedere nel contesto lavorativo norme specifiche sul trattamento dei dati personali dei dipendenti (cfr. L'articolo 88).

4. INFORMATIVA SU RIPRESE VIDEO A TERZI.

48. In linea di principio, per la divulgazione di registrazioni video a terzi si applicano le norme generali del GDPR.

4.1 Divulgazione di riprese video a terzi in generale.

49. La divulgazione è definita all'articolo 4, paragrafo 2, come trasmissione (ad es. Comunicazione individuale), diffusione (ad es. Pubblicazione online) o messa a disposizione in altro modo. Le terze parti sono definite nell'articolo 4, paragrafo 10. Laddove le informazioni vengano divulgate a paesi terzi o organizzazioni internazionali, si applicano anche le disposizioni particolari di cui agli articoli 44 e seguenti.

50. Qualsiasi divulgazione di dati personali è un tipo separato di trattamento di dati personali per il quale il Titolare del trattamento deve disporre di una base giuridica di cui all'articolo 6.

51.

Esempio: Un Titolare del trattamento che desidera caricare una registrazione su Internet deve fare affidamento su una base giuridica per tale trattamento, ad esempio ottenendo il consenso dell'interessato ai sensi dell'articolo 6, paragrafo 1, lettera a).

52. La trasmissione di riprese video a terzi per scopi diversi da quelli per i quali sono stati raccolti i dati è possibile ai sensi dell'articolo 6, paragrafo 4.

53.

Esempio: la videosorveglianza di una barriera (in un parcheggio) è installata per la finalità di risolvere i danni. Si verifica un danno e la registrazione viene trasferita a un avvocato per perseguire un caso. In questo caso la finalità della registrazione è la stessa di quella del trasferimento.

Esempio: la videosorveglianza di una barriera (in un parcheggio) è installata allo scopo di risolvere i danni. La registrazione è pubblicata online per puro divertimento. In questo caso la finalità è cambiata e non è compatibile con quella iniziale.

54. Un destinatario terzo dovrà effettuare la propria analisi giuridica, in particolare identificando per il suo trattamento la relativa base giuridica ai sensi dell'articolo 6 (ad esempio, la ricezione del materiale).

4.2 Divulgazione di riprese video alle Forze dell'Ordine.

55. Anche la divulgazione di registrazioni video alle forze dell'ordine è un processo indipendente, che richiede una giustificazione separata per il Titolare del trattamento.

56. Ai sensi dell'articolo 6, paragrafo 1, lettera c), il trattamento è legale se è necessario per adempiere ad un obbligo di legge a cui è soggetto il Titolare del trattamento. Sebbene la legge di polizia applicabile sia sotto il controllo esclusivo degli Stati membri, ci sono probabilmente in ogni stato membro regole generali che stabiliscono le modalità di trasferimento di prove alle forze dell'ordine. Tale trasferimento è un trattamento del Titolare ed è quindi regolato dal GDPR. Se la legislazione nazionale impone al Titolare del

trattamento di cooperare con le forze dell'ordine (ad es. un'indagine), la base giuridica per la consegna dei dati è un obbligo legale ai sensi dell'articolo 6, paragrafo 1, lettera c).

57. La limitazione delle finalità di cui all'articolo 6, paragrafo 4, è quindi spesso priva di problemi, poiché la divulgazione si rifà esplicitamente al diritto degli Stati membri. Una considerazione dei requisiti particolari per un cambiamento di finalità ai sensi delle lettere "a-e" non è quindi necessario.

58.

Esempio: un proprietario del negozio registra filmati al suo ingresso. Registra una persona che ruba il portafoglio di un'altra persona. La polizia chiede al Titolare del trattamento di consegnare il materiale video allo scopo di aiutarli nelle loro indagini. In questo caso il proprietario del negozio utilizzerà la base giuridica ai sensi dell'articolo 6, paragrafo 1, lettera c) (obbligo legale) interpretato in combinato con la normativa nazionale riguardante il trasferimento di quei dati.

Esempio: una videocamera è installata in un negozio per motivi di sicurezza. Il proprietario del negozio ritiene di aver registrato qualcosa di sospetto nel suo filmato e decide di inviare il materiale alla polizia (senza alcuna indicazione che siano in corso indagini di qualche tipo). In questo caso il proprietario del negozio deve valutare se sono soddisfatte le condizioni di cui all'articolo 6, paragrafo 1, lettera f).

59. Il trattamento dei dati personali da parte delle stesse forze dell'ordine non segue il GDPR (vedere l'articolo 2, paragrafo 2, lettera d)), ma segue invece la direttiva sull'applicazione della legge (EU 2016/680).

5. TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI.

60. I sistemi di videosorveglianza di solito raccolgono enormi quantità di dati personali che possono rivelare dati di natura altamente personale e persino categorie particolari di dati. In effetti, i dati apparentemente non significativi originariamente raccolti attraverso il video possono essere utilizzati per dedurre altre informazioni per raggiungere una finalità diversa (ad esempio per mappare le abitudini di un individuo). Tuttavia, la videosorveglianza non è sempre considerata un trattamento di categorie particolari di dati personali.

61.

Esempio: 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.

62. Tuttavia, se il filmato viene elaborato per ricavare categorie particolari di dati, si applica l'articolo 9.

63.

Esempio: potrebbero essere dedotte le opinioni politiche da immagini che mostrano soggetti identificabili che prendono parte a un evento, partecipano a uno sciopero, ecc.. Questo caso rientrerebbe nell'articolo 9.

Esempio: l'installazione da parte di un ospedale di una videocamera per monitorare le condizioni di salute di un paziente sarebbe considerato un trattamento di categorie particolari di dati personali (articolo 9).

64. In linea di principio, ogni volta che si installa un sistema di videosorveglianza si dovrebbe prestare particolare attenzione al principio di minimizzazione dei dati. Pertanto, anche nei casi in cui non si applica l'articolo 9, paragrafo 1, il Titolare del trattamento dei dati dovrebbe sempre cercare di ridurre al minimo il rischio di acquisire filmati rivelando altri dati particolari sensibili (a parte l'articolo 9), indipendentemente dalla finalità prevista.

65.

Esempio: una videosorveglianza che riprende una chiesa non rientra di per sé nell'applicazione dell'articolo 9. Tuttavia, il Titolare del trattamento deve condurre una valutazione particolarmente attenta ai sensi dell'articolo 6, paragrafo 1, lettera f), tenendo conto della natura dei dati e del rischio di acquisire altri dati particolari sensibili (a parte l'articolo 9) nel valutare il coinvolgimento della persona interessata.

66. Se un sistema di videosorveglianza è utilizzato per trattare categorie particolari di dati, il Titolare del trattamento dei dati deve valutare sia un'eccezione per il trattamento di categorie particolari di dati ai sensi dell'articolo 9 (vale a dire una deroga dalla regola generale che non si dovrebbero trattare categorie particolari di dati) che una base giuridica ai sensi dell'articolo 6.

67. Ad esempio, potrebbe - in teoria ed eccezionalmente - essere utilizzato l'articolo 9, paragrafo 2, lettera c) (il trattamento è necessario per proteggere gli interessi vitali dell'interessato o di un'altra persona fisica qualora l'interessato sia fisicamente o giuridicamente incapace di fornire il consenso), ma il Titolare del trattamento dei dati dovrebbe giustificarlo come una necessità assoluta per salvaguardare gli interessi vitali di una persona e dimostrare che questa persona "*è fisicamente o giuridicamente incapace di dare il proprio consenso*". Inoltre, al Titolare del trattamento non è consentito di utilizzare il sistema per altre finalità.

68.

Esempio: un ospedale sta monitorando un paziente per motivi medici. L'interessato è stato portato in ambulanza incosciente in ospedale. In questo caso potrebbe applicarsi l'articolo 9, paragrafo 2, lettera c).

69. È importante notare qui che per giustificare il trattamento di categorie particolari di dati attraverso la videosorveglianza non saranno probabilmente utilizzabili lei deroghe elencate nell'articolo 9. Più specificamente, i Titolari del trattamento dei dati che trattano tali dati nel contesto della videosorveglianza non possono fare affidamento sull'articolo 9, paragrafo 2, lettera e), che consente il trattamento relativo ai dati personali che sono manifestamente resi pubblici dall'interessato. Il semplice fatto di entrare nel raggio di azione della videocamera non implica che l'interessato intenda rendere pubbliche categorie particolari di dati che lo riguardano.

70. Inoltre, il trattamento di categorie particolari di dati richiede una vigilanza intensificata e continua nonché determinati obblighi; ad esempio una valutazione di alto livello dell'impatto sulla sicurezza e sulla protezione dei dati, ove necessario.

71.

Esempio: un datore di lavoro non deve utilizzare registrazioni di videosorveglianza che mostrano una manifestazione per identificare gli scioperanti.

5.1 Considerazioni generali in caso di trattamento di dati biometrici.

72. L'uso di dati biometrici e in particolare il riconoscimento facciale comportano maggiori rischi per i diritti degli interessati. È fondamentale che il ricorso a tali tecnologie avvenga nel rispetto dei principi di liceità, necessità, proporzionalità e minimizzazione dei dati stabiliti nel GDPR. Mentre l'uso di queste tecnologie può essere percepito come particolarmente efficace, i Titolari del trattamento dovrebbero innanzitutto valutare l'impatto sui diritti e sulle libertà fondamentali e considerare l'utilizzo di mezzi meno invasivi per raggiungere la loro legittima finalità del trattamento.

73. Per qualificarsi come dati biometrici definiti nel GDPR, il trattamento di dati grezzi non elaborati, come le caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, deve implicare una misurazione di queste caratteristiche. Poiché i dati biometrici sono il risultato di tali misurazioni, il GDPR afferma all'articolo 4 paragrafo 14 che " *i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*". Le riprese video di un individuo non possono tuttavia essere considerate di per sé come dati biometrici ai sensi dell'articolo 9, se non sono state trattate tecnicamente in modo specifico per contribuire all'identificazione di un individuo[16].

74. Affinché possa essere considerato il trattamento di categorie particolari di dati personali (articolo 9), è necessario che i dati biometrici siano trattati "per la finalità di identificare in modo univoco una persona fisica".

75. Per riassumere, alla luce dell'articolo 4 paragrafo 14 e dell'articolo 9, devono essere considerati tre criteri:

- **natura dei dati**: dati relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica,

- **mezzi e modalità del trattamento**: dati "derivanti da un trattamento tecnico specifico",

- **finalità del trattamento**: i dati devono essere utilizzati allo scopo di identificare in modo univoco una persona fisica.

76. L'uso della videosorveglianza che include la funzionalità di riconoscimento biometrico installato da soggetti privati per i propri scopi (ad es. marketing, statistica o anche sicurezza) richiederà, nella maggior parte dei casi, il consenso esplicito di tutte le persone interessate (articolo 9, paragrafo 2, lettera a)); tuttavia potrebbe essere applicabile anche un'altra eccezione all'articolo 9.

[16] Il Considerando 51 supporta questa analisi, affermando che " *Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica*".

77.

Esempio: per migliorare il proprio servizio, una società privata sostituisce i punti di controllo di identificazione dei passeggeri all'interno di un aeroporto (deposito 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 nell'articolo 9, i passeggeri, che in precedenza avranno dato il loro consenso esplicito e informato, dovranno registrarsi ad esempio presso un terminale automatico per creare e registrare il loro modello facciale associato alla carta d'imbarco e all'identità. I punti di controllo con riconoscimento facciale devono essere chiaramente separati: per esempio il sistema deve essere installato all'interno di un passaggio in modo che non vengano acquisiti i modelli biometrici delle persone che non hanno fornito il consenso. Solo i passeggeri che avranno precedentemente dato il loro consenso e proceduto alla loro iscrizione utilizzeranno l'apparecchiatura dotata del sistema biometrico.

Esempio: un Titolare gestisce l'accesso al suo edificio utilizzando un metodo di riconoscimento facciale. Le persone possono utilizzare questo modo di accesso solo se hanno prestato in precedenza un esplicito consenso informato (ai sensi dell'articolo 9, paragrafo 2, lettera a)). Tuttavia, al fine di garantire che nessuno che non abbia precedentemente prestato il proprio consenso sia acquisito, il metodo di riconoscimento facciale dovrebbe essere attivato dall'interessato stesso, ad esempio premendo un pulsante. Per garantire la liceità del trattamento, il Titolare del trattamento deve sempre offrire un modo alternativo per accedere all'edificio, senza trattamento biometrico, utilizzando magari badge o chiavi.

78. In questi casi in cui vengono generati modelli biometrici i controllori devono assicurare che una volta ottenuto il risultato di una corrispondenza o di una mancata corrispondenza, tutti i modelli intermedi realizzati al volo (con il consenso esplicito e informato dell'interessato) per confrontarli con quelli creati dagli interessati al momento della registrazione, vengano cancellati immediatamente e in modo sicuro. I modelli creati per la registrazione devono essere conservati solo sino alla realizzazione della finalità del trattamento e non devono essere memorizzati o archiviati.

79. Tuttavia, quando lo scopo del trattamento è, ad esempio, quello di distinguere una categoria di persone da un'altra ma di non identificare in modo univoco nessuno in particolare, il trattamento non rientra nell'articolo 9.

80.

Esempio: il proprietario di un negozio desidera personalizzare la propria pubblicità in base alle caratteristiche di genere e di età del cliente catturato da un sistema di videosorveglianza. Se tale sistema non genera modelli biometrici al fine di identificare in modo univoco le persone ma rileva invece solo quelle caratteristiche fisiche e di conseguenza la persona viene soltanto classificata, il trattamento non rientra nell'articolo 9.

81. Tuttavia, se il Titolare del trattamento memorizza i dati biometrici (più comunemente attraverso modelli creati dall'estrazione di caratteristiche chiave dalla forma grezza di dati biometrici, ad esempio misurazioni facciali da un'immagine) allo scopo di identificare in modo univoco una persona, si applica l'articolo 9. Se un Titolare del trattamento desidera rilevare una persona interessata che rientra nell'area o accede a un'altra area (ad esempio per proiettare annunci pubblicitari continui personalizzati), la finalità sarebbe quindi di identificare in modo univoco una persona fisica, il che significa che il trattamento rientrerebbe nell'articolo 9. Questo potrebbe accadere se un Titolare memorizza modelli generati per fornire ulteriori annunci pubblicitari su più cartelloni pubblicitari in diverse posizioni all'interno del negozio. Poiché il sistema utilizza le caratteristiche fisiche per rilevare individui specifici che rientrano nel raggio di azione della telecamera (come i visitatori di un centro commerciale) e per rintracciarli, costituirebbe un metodo di identificazione biometrica perché è finalizzato al riconoscimento attraverso l'utilizzo di specifici trattamenti tecnici.

82.

Esempio: il proprietario di un negozio ha installato un sistema di riconoscimento facciale nel suo negozio al fine di personalizzare la sua pubblicità verso gli avventori. Il Titolare del trattamento dei dati deve ottenere il consenso esplicito e informato di tutti gli interessati prima di utilizzare questo sistema biometrico e fornire pubblicità su misura. Il sistema sarebbe illegale se cattura visitatori o passanti che non hanno acconsentito alla creazione del loro modello biometrico, anche se il loro modello viene eliminato nel più breve tempo possibile. In effetti, questi modelli temporanei costituiscono dati biometrici trattati per la finalità di identificare in modo univoco una persona che potrebbe non voler ricevere pubblicità mirata.

83. L'EDPB osserva che alcuni sistemi biometrici sono installati in un ambiente non controllato[17], il che significa che il sistema prevede di catturare al volo le facce di qualsiasi individuo che passa nel raggio del dispositivo biometrico e quindi di creare modelli biometrici. Questi modelli vengono confrontati con quelli creati dagli interessati che hanno prestato il loro consenso preventivo durante un processo di iscrizione (ovvero un utente di dispositivi biometrici) in modo che il Titolare del trattamento dei dati possa riconoscere se la persona è un utente del dispositivo biometrico o meno. In questo caso, il sistema è spesso progettato per individuare le persone per riconoscere se sono archiviate in un database oppure no. Poiché lo scopo è identificare in modo univoco le persone fisiche, è ancora necessaria una deroga ai sensi dell'articolo 9, paragrafo 2, del GDPR per chiunque sia catturato dalla fotocamera.

84.

Esempio: un hotel utilizza la videosorveglianza per avvisare automaticamente il direttore dell'hotel che un VIP è arrivato quando viene riconosciuto il volto dell'ospite. Questi VIP hanno preventivamente dato il loro esplicito consenso all'uso del riconoscimento facciale prima di essere registrati in un database creato a tale scopo. Questi sistemi di trattamento dei 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.

Esempio: un gestore dei una sala da concerto installa un sistema di videosorveglianza con riconoscimento facciale all'ingresso. Il Titolare del trattamento deve impostare ingressi chiaramente separati; uno con un sistema biometrico e uno senza (dove invece per esempio avviene la scansione del 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.

85. Infine, quando il consenso è richiesto dall'articolo 9 del GDPR, il Titolare del trattamento dei dati non deve condizionare l'accesso ai suoi servizi all'accettazione del trattamento biometrico. In altre parole, in particolare quando il trattamento biometrico viene utilizzato per la finalità di autenticazione, il Titolare del trattamento dei dati deve offrire una soluzione alternativa che non preveda il trattamento biometrico, senza restrizioni o costi aggiuntivi per l'interessato. Questa soluzione alternativa è necessaria anche per le persone che non soddisfano i vincoli del dispositivo biometrico (impossibilità di registrazione o lettura dei dati biometrici, situazione di disabilità che ne rende difficile l'utilizzo, ecc.) e in previsione di indisponibilità del dispositivo biometrico (ad esempio come malfunzionamento del dispositivo), deve essere implementata una "soluzione di backup" per garantire la continuità del servizio proposto, limitato tuttavia a un uso eccezionale.

[17] Significa che il dispositivo biometrico si trova in uno spazio aperto al pubblico ed è in grado di lavorare su chiunque passi, al contrario dei sistemi biometrici in ambienti controllati che possono essere utilizzati solo da parte di persone che hanno fornito il consenso.

5.2 Misure suggerite per ridurre al minimo i rischi nel trattamento di dati biometrici.

86. In ottemperanza al principio di minimizzazione dei dati, i Titolari del trattamento dei dati devono garantire che i dati estratti da un'immagine digitale per costruire un modello non siano eccessivi e conterranno solo le informazioni richieste per la finalità specificata, evitando così ogni possibile ulteriore trattamento. Dovrebbero essere messe in atto misure per garantire che i modelli non possano essere trasferiti attraverso sistemi biometrici.

87. È probabile che l'identificazione e l'autenticazione/verifica richiedano la memorizzazione del modello per un successivo confronto. Il Titolare del trattamento dei dati deve considerare la gestione più idonea per l'archiviazione dei dati. In un ambiente sotto controllo (corridoi o punti di controllo delimitati), i modelli devono essere memorizzati su un singolo dispositivo tenuto dall'utente e sotto il suo esclusivo controllo (in uno smartphone o la carta d'identità) o - quando necessario per scopi specifici e in presenza di esigenze oggettive - memorizzato in un database centralizzato in forma crittografata con una chiave segreta esclusivamente nelle mani della persona, per impedire l'accesso non autorizzato al modello o alla sua posizione di archiviazione. Se il Titolare del trattamento dei dati non può evitare di accedere ai modelli, deve adottare misure idonee per garantire la sicurezza dei dati memorizzati. Ciò può includere la crittografia del modello mediante un algoritmo crittografico.

88. In ogni caso, il Titolare del trattamento prende tutte le precauzioni necessarie per preservare la disponibilità, l'integrità e la riservatezza dei dati trattati. A tal fine, il Titolare del trattamento adotta in particolare le seguenti misure: ripartire i dati durante la trasmissione e l'archiviazione, archiviare modelli biometrici e dati grezzi o dati di identità su database distinti, crittografare i dati biometrici, in particolare i modelli biometrici, e definire una politica per la crittografia e la gestione delle chiavi, implementare una misura organizzativa e tecnica per il rilevamento delle frodi, associare un codice di integrità ai dati (ad esempio firma o hash) e vietare qualsiasi accesso esterno ai dati biometrici.

89. Inoltre i Titolari del trattamento dei dati devono procedere alla cancellazione dei dati grezzi (immagini del viso, segnali vocali, andatura, ecc.) e garantire l'efficacia di tale cancellazione. Infatti, nella misura in cui i modelli biometrici derivano da tali dati, si può considerare che la costituzione di database potrebbe rappresentare una minaccia uguale se non addirittura maggiore (perché potrebbe non essere sempre facile leggere un modello biometrico senza la conoscenza di come è stato programmato, mentre i dati non trattati costituiranno la base di qualsiasi modello). Nel caso in cui il Titolare del trattamento dei dati debba conservare tali dati, è necessario esplorare il metodo di aggiunta del rumore (come la filigrana), il che renderebbe inefficace la creazione del modello. Il controllore deve anche eliminare i dati e i modelli biometrici in caso di accesso non autorizzato al terminale di lettura/controllo o al server di archiviazione ed eliminare tutti i dati non utili per un ulteriore trattamento al termine della vita del dispositivo biometrico.

6. DIRITTI DEGLI INTERESSATI.

90. A causa della particolarità del trattamento dei dati quando si utilizza la videosorveglianza, servono ulteriori chiarimenti sui diritti dell'interessato ai sensi del GDPR. Questo capitolo non è tuttavia esaustivo, e tutti i diritti previsti dal GDPR si applicano anche al trattamento dei dati personali attraverso la videosorveglianza.

6.1 Diritto di accesso.

91. L'interessato ha il diritto di ottenere la conferma dal Titolare del trattamento in merito al trattamento o meno dei propri dati personali. Per la videosorveglianza ciò significa che una volta trascorso il momento di monitoraggio in tempo reale se nessun dato viene archiviato o trasferito in alcun modo, il Titolare del trattamento potrebbe solo fornire l'informazione che nessun dato personale verrà più trattato (oltre agli obblighi di informazione generali di cui all'articolo 13, *vedere la sezione 7 - Trasparenza e obblighi di informazione*). Se tuttavia i dati sono ancora in fase di trattamento al momento della richiesta (vale a dire se i dati sono archiviati o continuano ad essere trattati in un altro modo), l'interessato dovrebbe ricevere accesso alle informazioni ai sensi dell'articolo 15.

92. Vi sono tuttavia alcune limitazioni che in alcuni casi possono essere applicate in relazione al diritto di accesso.

- L'articolo 15, paragrafo 4 del GDPR incide negativamente sui diritti di terzi.

93. Può accadere comunque che nella stessa sequenza di videosorveglianza possa essere registrato un numero qualunque di soggetti interessati, che causerebbe quindi un trattamento aggiuntivo dei dati personali di altre persone interessate. Se l'interessato desidera ricevere una copia del materiale (articolo 15, paragrafo 3), ciò potrebbe influire negativamente sui diritti e sulle libertà di altre persone interessate presenti nel video. Per evitare tale effetto, il Titolare dovrebbe pertanto tenere presente che, a causa della natura invasiva del filmato, il Titolare del trattamento non dovrebbe in alcuni casi distribuire filmati in cui è possibile identificare altri soggetti. La protezione dei diritti di terzi non dovrebbe tuttavia essere utilizzata come una scusa per prevenire legittime richieste di accesso da parte di individui e il Titolare del trattamento dovrebbe invece implementare misure tecniche per soddisfare la richiesta di accesso (ad esempio, modifica delle immagini con funzioni di mascheramento o annebbiamento).

- Articolo 11, paragrafo 2 del GDPR: il Titolare del trattamento non è in grado di identificare l'interessato.

94. Se il filmato non è rintracciabile tra i dati personali, (vale a dire che il Titolare del trattamento dovrebbe probabilmente passare attraverso una grande quantità di materiale archiviato per trovare l'interessato in questione), il Titolare del trattamento potrebbe non essere in grado di identificare l'interessato.

95. Per questi motivi l'interessato nella sua richiesta al Titolare del trattamento dovrebbe (oltre a identificarsi con un documento di identità o di persona), specificare quando - entro un termine ragionevole in proporzione alla quantità di soggetti registrati - è entrato nell'area monitorata. Il Titolare del trattamento deve comunicare preventivamente all'interessato quali informazioni sono necessarie affinché il Titolare del trattamento possa soddisfare la richiesta. Di conseguenza se il Titolare del trattamento è in grado di dimostrare di non essere in grado di identificare l'interessato, il medesimo Titolare deve se possibile informare l'interessato.

96.

Esempio: se l'interessato richiede una copia dei propri dati personali trattati attraverso la videosorveglianza all'ingresso di un centro commerciale con 30.000 visitatori al giorno, dovrebbe specificare quando ha attraversato l'area monitorata fornendo un intervallo di circa 1-2 ore. Se il Titolare tratta ancora i dati registrati, deve fornire una copia del filmato. Se a nello stesso video possono essere identificate altre persone interessate, tale parte del video deve essere anonimizzato (ad esempio sfocando la copia o parti di essa) prima di consegnare la copia all'interessato che ha presentato la richiesta.

Esempio: se il Titolare cancella automaticamente tutte le riprese, ad esempio entro 2 giorni, se l'interessato presenta la richiesta al Titolare dopo quei 2 giorni avrà come risposta che i dati sono stati eliminati.

- Articolo 12 del GDPR: richieste eccessive.

97. In caso di richieste eccessive o manifestamente infondate da parte dell'interessato, il Titolare del trattamento può addebitare un costo ragionevole ai sensi dell'articolo 12, paragrafo 5, lettera a), del Regolamento Generale sulla Protezione dei Dati o rifiutare di dare seguito alla richiesta (articolo 12, paragrafo 5, lettera b) GDPR. Il Titolare del trattamento deve essere in grado di dimostrare il carattere eccessivo o manifestamente infondato della richiesta.

6.2 Diritto alla cancellazione e diritto di opposizione.

6.2.1 Diritto alla cancellazione (Diritto all'oblio)

98. Se il Titolare del trattamento continua a trattare i dati personali dopo il monitoraggio in tempo reale (ad esempio memorizzando il video) l'interessato può richiedere la cancellazione dei dati personali ai sensi dell'articolo 17 del GDPR.

99. Su richiesta, il Titolare del trattamento è tenuto a cancellare i dati personali senza indebito ritardo se si applica una delle circostanze elencate nell'articolo 17 paragrafo 1 del GDPR (e non rientra nelle eccezioni elencate nell'articolo 17 paragrafo 3 del GDPR). Ciò include l'obbligo di cancellare i dati personali quando non sono più necessari per la finalità per cui sono stati inizialmente memorizzati o quando il trattamento è illegale (vedere anche la sezione 8 sui periodi di conservazione e l'obbligo di cancellazione). Inoltre, a seconda della base giuridica del trattamento, i dati personali devono essere cancellati:

- per il consenso ogni volta che il consenso viene revocato (e non esiste altra base giuridica per il trattamento)

- per legittimo interesse:
  - ogni volta che l'interessato esercita il diritto di opposizione (vedere la sezione 6.2.2) e non vi sono motivi legittimi convincenti e prevalenti per il trattamento, o
  - in caso di marketing diretto (compresa la profilazione) ogni volta che l'interessato si oppone al trattamento.

100. Se il Titolare del trattamento ha reso pubbliche le riprese video (ad es. Trasmissione o streaming online), è necessario adottare misure ragionevoli per informare gli altri Titolari del trattamento (che stanno attualmente trattando i dati personali in questione) della richiesta ai sensi dell'articolo 17, paragrafo 2 del GDPR. Le misure ragionevoli dovrebbero includere misure tecniche, tenendo conto della tecnologia disponibile e dei costi di attuazione. Nella misura possibile, il Titolare del trattamento dovrebbe

comunicare - in caso di cancellazione dei dati personali – i soggetti a cui i dati personali siano stati precedentemente divulgati, ai sensi dell'articolo 19 del GDPR.

101. Il Titolare del trattamento oltre all'obbligo di cancellare i dati personali in caso di richiesta dell'interessato, è tenuto, in base ai principi generali del GDPR, a limitare i dati personali memorizzati (vedere la sezione 8).

102. Per la videosorveglianza vale la pena notare che, ad esempio, sfocando l'immagine senza alcuna capacità retroattiva di recuperare i dati personali dell'immagine precedentemente contenuta, i dati personali sono considerati cancellati in conformità con il GDPR.

103.

Esempio: un negozio di alimentari ha problemi con atti di vandalismo in particolare al suo esterno e quindi utilizza la videosorveglianza al di fuori dell'ingresso installando le videocamere sulle pareti esterne. Un passante chiede di cancellare i suoi dati personali da quel momento. Il Titolare del trattamento è tenuto a rispondere alla richiesta senza indebito ritardo e al più tardi entro un mese. Poiché il filmato in questione non soddisfa più la finalità per cui è stato inizialmente archiviato (non si sono verificati atti di vandalismo durante il periodo in cui l'interessato è passato), al momento della richiesta non esiste alcun interesse legittimo a continuare a memorizzare i dati che potrebbero prevalere sui diritti degli interessati. Il Titolare del trattamento deve cancellare i dati personali.

6.2.2 Diritto di opposizione.

104. Per la videosorveglianza basata sull'interesse legittimo (articolo 6, paragrafo 1, lettera f) del GDPR) oppure sulla necessità di svolgere un compito di interesse pubblico (articolo 6, paragrafo 1, lettera e) del GDPR) l'interessato ha diritto in qualsiasi momento, per motivi relativi alla sua situazione particolare, di opporsi al trattamento ai sensi dell'articolo 21 del GDPR. A meno che il Titolare del trattamento non dimostri validi motivi legittimi che prevalgono sui diritti e sugli interessi della persona interessata, deve quindi essere interrotto il trattamento dei dati della persona che ha contestato. Il Titolare del trattamento è tenuto a rispondere alle richieste dell'interessato senza indebito ritardo e al più tardi entro un mese.

105. Nel contesto della videosorveglianza, questa opposizione potrebbe essere fatta prima di entrare, durante la permamenza o dopo aver lasciato l'area monitorata. In pratica ciò significa che, a meno che il Titolare del trattamento non abbia validi motivi legittimi, il monitoraggio di un'area in cui le persone fisiche potrebbero essere identificate è lecito solo se:

(1) il Titolare del trattamento è in grado di interrompere immediatamente il trattamento dei dati personali da parte della telecamera quando richiesto, oppure

(2) l'area monitorata è così limitata che il Titolare del trattamento possa garantire l'approvazione dell'interessato prima di entrare nell'area, e che non è un'area in cui l'interessato come cittadino ha diritto di accedere.

106. Quando si utilizza la videosorveglianza per scopi di marketing diretto, l'interessato ha il diritto di opporsi al trattamento su base discrezionale in quanto il diritto di opposizione è assoluto in tale contesto (articolo 21, paragrafi 2 e 3 del GDPR).

107.

Esempio: un'azienda sta incontrando difficoltà con violazioni della sicurezza all'ingresso del pubblico e utilizza la videosorveglianza per motivi di legittimo interesse, con la finalità di registrare coloro che entrano illegalmente. Un visitatore si oppone al trattamento dei propri dati attraverso il sistema di videosorveglianza per motivi relativi alla propria situazione particolare. Tuttavia, in questo caso la società rifiuta la richiesta con la spiegazione che il filmato è necessario a causa di un'indagine interna in corso, quindi esistono validi motivi legittimi per continuare a trattare i dati personali.

7 OBBLIGHI DI TRASPARENZA E INFORMAZIONI[18].

108. È dai tempi della legge europea sulla protezione dei dati che gli interessati dovrebbero essere resi consapevoli del fatto che la videosorveglianza è in funzione. Essi dovrebbero essere informati in modo dettagliato in merito ai luoghi monitorati[19]. Ai sensi del GDPR, gli obblighi generali in materia di trasparenza e informazione sono stabiliti dall'articolo 12 del GDPR e seguenti. Gli "Orientamenti sulla trasparenza ai sensi del regolamento 2016/679 (WP260) del Gruppo di lavoro Articolo 29", approvati dall'EDPB il 25 maggio 2018, forniscono ulteriori dettagli. In linea con il paragrafo WP260. 26 è l'articolo 13 del GDPR, che è applicabile se i dati personali sono raccolti "da una persona interessata mediante osservazione (ad esempio utilizzando dispositivi di acquisizione dati automatizzati o software di acquisizione dati tramite telecamere)".

109. Alla luce del volume di informazioni che è necessario fornire all'interessato, i Titolari del trattamento possono seguire un approccio a più livelli in cui scelgono di utilizzare una combinazione di metodi per garantire la trasparenza (WP260, paragrafo 35; WP89, paragrafo 22). Per quanto riguarda la videosorveglianza, le informazioni più importanti dovrebbero essere visualizzate sul segnale di avvertimento stesso (primo livello) mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello).

7.1 Informazioni di primo livello (segnale di avvertimento)

110. Il primo livello riguarda il modo principale con cui il Titolare del trattamento si impegna per la prima volta con l'interessato. In questa fase si possono utilizzare segnali di avvertimento che mostrano le informazioni pertinenti. Le informazioni visualizzate possono essere fornite in combinazione con un'icona al fine di fornire, in modo facilmente visibile, comprensibile e chiaramente leggibile, una panoramica significativa del trattamento previsto (articolo 12, paragrafo 7del GDPR). Il formato delle informazioni deve essere adattato alla singola posizione (WP89 paragrafo 22).

7.1.1 Posizionamento del segnale di avvertimento.

111. Le informazioni dovrebbero essere posizionate a una distanza ragionevole dai luoghi monitorati (WP 89, paragrafo 22) in modo tale che l'interessato possa facilmente riconoscere l'esistenza della videosorveglianza prima di entrare nell'area monitorata (approssimativamente a livello degli occhi). Non è necessario specificare l'ubicazione precisa delle apparecchiature di sorveglianza purché non vi siano dubbi, su quali aree siano soggette a monitoraggio e sia chiaro in modo inequivocabile il contesto della sorveglianza (WP 89, p. 22). L'interessato deve essere in grado di stimare quale area è acquisita da una telecamera in modo da poter evitare la sorveglianza o adattare il suo comportamento, se necessario.

[18] Nelle legislazioni nazionali potrebbero essere applicati requisiti specifici.

[19] Gruppo di lavoro Articolo 29, parere 4/2004 sul trattamento dei dati personali mediante videosorveglianza (WP89).

7.1.2 Contenuti di primo livello.

112. Le informazioni di primo livello (segnale di avvertimento) dovrebbero in genere trasmettere le informazioni più importanti, ad esempio i dettagli delle finalità del trattamento, l'identità del Titolare del trattamento e l'esistenza dei diritti dell'interessato, insieme alle informazioni sui maggiori impatti del trattamento[20]. Ciò può includere, ad esempio, gli interessi legittimi perseguiti dal Titolare del trattamento (o da una terza parte) e i dettagli di contatto del Titolare della Protezione dei Dati (se applicabile). Deve anche fare riferimento alle informazioni più dettagliate di secondo livello e dove e come trovarle.

113. Inoltre, il segnale dovrebbe contenere anche tutte le informazioni che potrebbero impressionare l'interessato (WP260, paragrafo 38). Ad esempio, potrebbero essere la trasmissione dei dati a terzi, in particolare se si trovano al di fuori dell'UE, o il relativo periodo di conservazione. Se queste informazioni non sono indicate, l'interessato dovrebbe presumere che esiste solo un monitoraggio in tempo reale (senza alcuna registrazione o trasmissione di dati a terzi).

114.

Esempio:

[20] Vedi WP260, paragrafo 38.

7.2 Informazioni di secondo livello

115. Devono essere rese disponibili anche le informazioni di secondo livello, in un luogo facilmente accessibile all'interessato, come un foglio informativo completo disponibile in una posizione centrale (ad esempio banco informazioni, reception o cassiere) o visualizzato su un cartello facilmente accessibile. Come accennato in precedenza, il segnale di avvertimento di primo livello deve fare chiaramente riferimento alle informazioni di secondo livello. Inoltre, è meglio se le informazioni del primo livello fanno riferimento a una fonte digitale (ad esempio QR-code o indirizzo di un sito Web) delle informazioni di secondo livello. Tuttavia, le informazioni dovrebbero essere facilmente disponibili anche in modo non digitale. In ogni caso, deve essere possibile accedere alle informazioni di secondo livello senza entrare nell'area rilevata. Ciò può essere ottenuto, ad esempio, tramite un collegamento o qualsiasi altro mezzo appropriato come un numero di telefono a cui poter chiamare. Le informazioni devono contenere tutte le altre informazioni obbligatorie ai sensi dell'articolo 13 del GDPR.

116. Anche per renderle più efficaci, oltre a queste opzioni l'EDPB promuove l'uso di mezzi tecnologici per fornire le informazioni agli interessati. Questo può includere ad esempio la geolocalizzazione delle telecamere e l'inclusione di informazioni di mappatura nelle App o nei siti Web in modo che le persone possano facilmente identificare le relative fonti video, avere dettagli sull'esercizio dei propri diritti e, dall'altro, ottenere informazioni più dettagliate sulle modalità di trattamento.

117.

Esempio: il proprietario di un negozio sta monitorando il suo negozio. Per adeguarsi 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 del secondo livello presso la cassa o qualsiasi altra posizione centrale e facilmente accessibile del suo negozio.

8. PERIODI DI CONSERVAZIONE E OBBLIGO DI CANCELLAZIONE.

118. I dati personali non possono essere conservati più a lungo di quanto necessario per le finalità per le quali essi sono trattati (articolo 5 paragrafo 1 lettere c) ed e) del GDPR). In alcuni Stati membri potrebbero essere previste disposizioni specifiche per i periodi di conservazione in relazione alla videosorveglianza ai sensi dell'articolo 6, paragrafo 2, del GDPR.

119. Si deve verificare in tempi ristretti se è necessaria o meno l'archiviazione dei dati personali. In generale, per la videosorveglianza la protezione della proprietà o la conservazione delle prove sono spesso finalità legittime. Di solito i danni che si verificano possono essere controllati entro uno o due giorni. Tenendo conto dei principi di cui all'articolo 5, paragrafo 1, lettere c) ed e), del GDPR, in particolare la minimizzazione dei dati e la limitazione della conservazione, nella maggior parte dei casi i dati personali (ad esempio ai fini della rilevazione di atti di vandalismo) dovrebbero essere cancellati, idealmente automaticamente, dopo pochi giorni. Più è lungo il periodo di conservazione (in particolare se oltre le 72 ore), più devono essere fornite argomentazioni sulla legittimità della finalità e sulla necessità della conservazione. Se il proprietario utilizza la videosorveglianza non solo per monitorare in tempo reale i propri locali, ma intende anche archiviare i dati, e deve garantire che l'archiviazione sia effettivamente necessaria per il raggiungimento delle finalità. In tal caso, il periodo di conservazione deve essere chiaramente definito e impostato individualmente per ogni ciascuna finalità. È compito del Titolare del trattamento definire il periodo di conservazione adeguandosi ai principi di necessità e proporzionalità e dimostrare la conformità con le disposizioni del GDPR.

120.

Esempio: un proprietario di un piccolo negozio di norma si accorge di eventuali atti di vandalismo lo stesso giorno in cui si verificano. Di conseguenza, è sufficiente un periodo di conservazione regolare di 24 ore. I fine settimana chiusi o festivi potrebbero tuttavia essere motivi per un periodo di conservazione più lungo. Se viene rilevato un danno, potrebbe essere necessario archiviare il filmato per un periodo più lungo al fine di intraprendere un'azione legale contro l'autore del reato.

9. MISURE TECNICHE E ORGANIZZATIVE.

121. Come indicato nell'articolo 32, paragrafo 1 del GDPR, non solo il trattamento dei dati personali della videosorveglianza deve essere legalmente consentito, ma i Titolari e i Responsabili del trattamento devono anche fornire adeguate garanzie. Le misure organizzative e tecniche attuate devono essere proporzionali ai rischi per i diritti e le libertà delle persone fisiche, derivanti da distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso ai dati di videosorveglianza. Ai sensi degli articoli 24 e 25 del Regolamento generale sulla protezione dei dati, i Titolari del trattamento devono attuare misure tecniche e organizzative anche per salvaguardare tutti i principi di protezione dei dati durante il trattamento e stabilire i mezzi affinché gli interessati possano esercitare i propri diritti come definiti negli articoli da 15 a 22 del Regolamento Generale sulla protezione dei dati. I Titolari del trattamento dei dati dovrebbero adottare un quadro interno e le politiche che possano garantire tale attuazione sia al momento della determinazione dei mezzi per il trattamento sia al momento del trattamento stesso, compresa l'esecuzione delle valutazioni di impatto sulla protezione dei dati, quando necessario.

9.1 Panoramica sui sistemi di videosorveglianza.

Un sistema di videosorveglianza (VSS)[21] è costituito da dispositivi analogici e digitali e da software allo scopo di catturare immagini di una scena, gestirle e mostrarle a un operatore. I suoi componenti sono raggruppati nelle seguenti categorie:

- Ambiente video: acquisizione di immagini, interconnessioni e gestione delle immagini:
    - lo scopo dell'acquisizione di immagini è la generazione di un'immagine del mondo reale in un formato tale da poter essere utilizzata dal resto del sistema;
    - le interconnessioni descrivono tutta la trasmissione di dati all'interno dell'ambiente video, ovvero connessioni e comunicazioni. Esempi di connessioni sono cavi, reti digitali e trasmissioni wireless. Le comunicazioni descrivono tutti i segnali di dati video e di controllo, che possono essere digitali o analogici;
    - la gestione delle immagini include l'analisi, la memorizzazione e la visualizzazione 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 comprende la gestione dei comandi dell'operatore e le attività generate dal sistema (procedure di allarme, operatori di allarme);

[21] Il GDPR non fornisce una definizione per esso; una descrizione tecnica può ad esempio essere trovata nel documento EN 62676-1-1: 2014 Sistemi di videosorveglianza per l'uso in applicazioni di sicurezza - Parte 1-1: Requisiti di sistema video.

- le interfacce con altri sistemi potrebbero includere la connessione ad altri sistemi di sicurezza (controllo accessi, allarme antincendio) o non correlate alla sicurezza (sistemi di gestione degli edifici, riconoscimento automatico delle targhe)

- La sicurezza di un sistema VSS consiste nella riservatezza, integrità e disponibilità del sistema e dei dati:
  - la sicurezza del sistema include la sicurezza fisica di tutti i componenti del sistema e il controllo dell'accesso al VSS;
  - la sicurezza dei dati include la prevenzione della perdita o della manipolazione dei dati.

122.

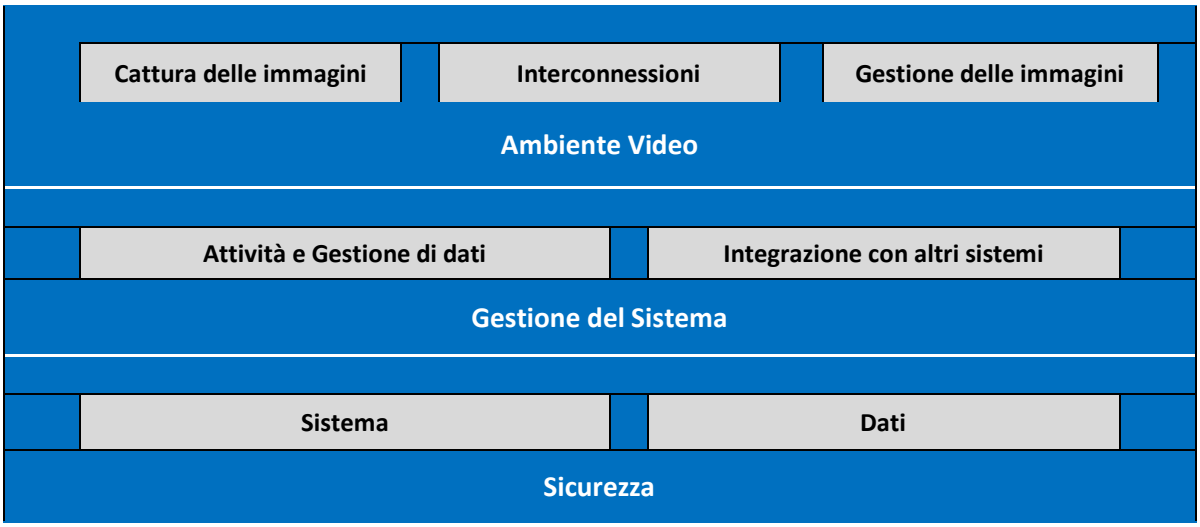

Figura 1- Sistema di Videosorveglianza

9.2 Data protection *by design* e *by default*

123. Come indicato nell'articolo 25 del GDPR, i Titolari del trattamento devono attuare misure tecniche e organizzative adeguate alla protezione dei dati non appena pianificano la videosorveglianza, prima di iniziare la raccolta e il trattamento dei filmati video. Questi principi sottolineano la necessità di tecnologie integrate per il miglioramento della privacy, impostazioni predefinite che riducono al minimo il trattamento dei dati e la fornitura degli strumenti necessari che consentano la massima protezione possibile dei dati personali[22].

124. I Titolari del trattamento dovrebbero applicare la protezione dei dati e la tutela della privacy non solo nelle specifiche di progettazione della tecnologia, ma anche nelle pratiche organizzative. Quando si tratta di pratiche organizzative, il Titolare del trattamento dovrebbe adottare un quadro di gestione adeguato, stabilire e applicare politiche e procedure relative alla videosorveglianza. Dal punto di vista tecnico, le specifiche e la progettazione del sistema dovrebbero includere i requisiti per il trattamento dei dati personali in conformità con i principi di cui all'articolo 5 GDPR (liceità del trattamento, finalità e limitazione dei dati, minimizzazione dei dati per impostazione predefinita ai sensi dell'articolo 25, paragrafo 2 GDPR, integrità e riservatezza, responsabilità ecc.). Nel caso in cui un Titolare preveda di acquisire un sistema di videosorveglianza in commercio, egli deve includere questi requisiti nelle

[22] Parere 168 del WP sul tema "Il futuro della privacy", contributo congiunto del Gruppo di lavoro sulla protezione dei dati ai sensi dell'articolo 29 e del Gruppo di lavoro sulla Polizia e la Giustizia alla consultazione della Commissione Europea sul quadro giuridico per il diritto fondamentale alla protezione dei dati personali (adottato il 01 dicembre 2009), https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

specifiche di acquisto. Il Titolare deve garantire la conformità a questi requisiti applicandoli a tutti i componenti del sistema e a tutti i dati trattati dallo stesso, durante l'intero ciclo di vita.

9.3 Esempi concreti di misure adeguate.

125. La maggior parte delle misure che possono essere utilizzate per proteggere la videosorveglianza, specialmente quando si utilizzano apparecchiature e software digitali, non differiranno da quelle utilizzate in altri sistemi IT. Tuttavia, indipendentemente dalla soluzione selezionata, il Titolare deve proteggere adeguatamente tutti i componenti di un sistema di videosorveglianza e i dati in tutte le fasi, vale a dire durante la memorizzazione (dati a riposo), la trasmissione (dati in transito) e l'elaborazione (dati in uso). Per questo, è necessario che Responsabili e Tecnici integrino misure organizzative e tecniche.

126. Quando si valutano soluzioni tecniche, il Titolare del trattamento dovrebbe prendere in considerazione tecnologie rispettose della privacy anche perché migliorano la sicurezza. Esempi di tali tecnologie sono i sistemi che consentono, quando si forniscono riprese video a soggetti interessati[23], di mascherare o annebbiare aree non rilevanti per la sorveglianza o di modificare le immagini di terze persone. D'altra parte, le soluzioni scelte non dovrebbero fornire funzioni che non sono necessarie (ad es. movimento illimitato di telecamere, capacità di zoom, trasmissione radio, analisi e registrazioni audio). Devono essere disattivate le funzionalità disponibili ma non necessarie.

127. Su questo argomento c'è molta letteratura disponibile, inclusi gli standard internazionali e le specifiche tecniche sulla sicurezza fisica dei sistemi multimediali[24] e la sicurezza dei sistemi IT in generale[25]. Pertanto, questa sezione fornisce su questo argomento solo una panoramica di alto livello.

9.3.1 Misure organizzative.

128. Oltre a un potenziale DPIA necessario (vedere la sezione 10), i Titolari del trattamento dovrebbero considerare i seguenti argomenti quando creano le proprie politiche e procedure di videosorveglianza:

- chi è Responsabile della gestione e del funzionamento del sistema di videosorveglianza;
- le finalità e la portata del progetto di videosorveglianza;
- l'uso appropriato e l'uso vietato (dove e quando è consentita la videosorveglianza e dove e quando non lo è; ad esempio l'uso di telecamere nascoste e la registrazione audio oltre che video[26]);
- le misure di trasparenza di cui alla sezione 7 (Trasparenza e obblighi di informazione);
- come viene registrato il video e per quale durata, incluso l'archiviazione delle registrazioni video relative a incidenti di sicurezza;

[23] In alcuni casi l'utilizzo di tali tecnologie può anche essere obbligatorio per conformarsi all'articolo 5, paragrafo 1, lettera c). In ogni caso possono servire come esempi di buone pratiche.

[24] IEC TS 62045 - Sicurezza multimediale - Linee guida per la protezione della privacy di apparecchiature e sistemi in uso e fuori uso.

[25] ISO/IEC 27000 - Serie di sistemi per la gestione della sicurezza delle informazioni.

[26] Ciò può dipendere dalle leggi nazionali e dalle normative di settore.

- chi deve seguire una formazione pertinente e quando;

  chi ha accesso alle registrazioni video e per quali finalità;

- le procedure operative (ad es. da chi e da dove viene monitorata la videosorveglianza, cosa fare in caso di incidente oi violazione dei dati);

- quali procedure devono seguire le parti esterne per richiedere le registrazioni video e le procedure per rifiutare o accogliere tali richieste;

- le procedure per l'approvvigionamento, l'installazione e la manutenzione di VSS;

- le procedure di gestione e recupero degli incidenti.

9.3.2 Misure tecniche.

129. **Sicurezza del sistema** significa sicurezza fisica di tutti i componenti del sistema, integrità del sistema, ovvero **protezione e resilienza in caso di interferenza intenzionale e non intenzionale con le sue normali operazioni e il controllo degli accessi**. Sicurezza dei dati significa **riservatezza** (i dati sono accessibili solo a coloro che sono autorizzati all'accesso), **integrità** (prevenzione contro la perdita o la manipolazione dei dati) e **disponibilità** (possibilità di accedervi quando è necessario).

130. La sicurezza fisica è una parte vitale della protezione dei dati e la prima linea di difesa, perché protegge le apparecchiature VSS da furti, atti vandalici, calamità naturali, catastrofi causate dall'uomo e danni accidentali (ad esempio, da sovratensioni elettriche, temperature estreme o caffè versato). Nel caso di sistemi analoghi, la sicurezza fisica svolge il ruolo principale nella loro protezione.

131. **La sicurezza del sistema e dei dati**, ovvero la protezione da interferenze intenzionali e non intenzionali durante la normale attività può includere:

- protezione dell'intera infrastruttura VSS (comprese telecamere remote, cavi e alimentatore) contro manomissioni fisiche e furti;

- protezione della trasmissione di filmati con canali di comunicazione sicuri contro l'intercettazione;

- crittografia dei dati;

- utilizzo di soluzioni basate su hardware e software come firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici;

- rilevamento di guasti di componenti, software e interconnessioni;

- mezzi per ripristinare la disponibilità e l'accesso al sistema in caso di incidente fisico o tecnico.

Il controllo degli accessi garantisce che solo le persone autorizzate possano accedere al sistema e ai dati, mentre viene impedito agli altri di farlo. Le misure che supportano il controllo dell'accesso fisico e logico includono:

- garantire che tutti i locali in cui viene effettuato il monitoraggio della videosorveglianza e vengono archiviate le riprese video siano protetti contro l'accesso non controllato da parte di terzi;

- posizionamento dei monitor (specialmente quando si trovano in aree aperte, come presso una reception) in modo tale che possano visualizzarli solo gli operatori autorizzati;

- sono definite e applicate le procedure per la concessione, la modifica e la revoca dell'accesso fisico e logico;

- sono implementati metodi e mezzi di autenticazione e autorizzazione dell'utente, incluso ad esempio la lunghezza delle password e la frequenza di modifica;

- vengono registrate e riviste periodicamente le azioni eseguite dall'utente (sia sul sistema che sui dati);

- il monitoraggio e il rilevamento degli errori di accesso vengono effettuati in modo continuo e le carenze rilevate vengono affrontate al più presto.

10. DPIA (DATA PROTECTION IMPACT ASSESSMENT).

132. Ai sensi dell'articolo 35, paragrafo 1, i Titolari sono tenuti a effettuare le valutazioni d'impatto sulla protezione dei dati (DPIA) quando un tipo di trattamento dei dati può comportare un rischio elevato per i diritti e la libertà delle persone fisiche. L'articolo 35, paragrafo 3, lettera c) del GDPR stabilisce che i Titolari del trattamento sono tenuti a effettuare valutazioni d'impatto sulla protezione dei dati se il trattamento costituisce un monitoraggio sistematico di un'area accessibile al pubblico su larga scala. Inoltre, ai sensi dell'articolo 35, paragrafo 3, lettera b), del Regolamento Europeo sulla protezione dei dati, quando il Titolare del trattamento intende trattare categorie particolari di dati su larga scala è necessaria anche una valutazione d'impatto sulla protezione dei dati.

133. Le Linee guida sulla valutazione d'impatto sulla protezione dei dati forniscono ulteriori consigli e esempi più rilevanti e dettagliati per la videosorveglianza (ad esempio, riguardanti "l'uso di un sistema di telecamere per monitorare il comportamento di guida in autostrada"). L'articolo 35, paragrafo 4, del Regolamento Europeo sulla protezione dei dati richiede che ciascuna Autorità di controllo pubblichi un elenco del tipo di operazioni di trattamento soggette obbligatoriamente al DPIA nel proprio Paese. Questi elenchi sono generalmente disponibili sui siti Web delle Autorità. Date le finalità tipiche della videosorveglianza (protezione delle persone e delle proprietà, individuazione, prevenzione e controllo dei reati, raccolta di prove e identificazione biometrica di sospetti), è ragionevole presumere che molti casi di videosorveglianza richiederanno una DPIA. Pertanto, i Titolari del trattamento dei dati dovrebbero consultare attentamente questi documenti al fine di determinare se tale valutazione sia necessaria e se è necessario implementarla. Il risultato della DPIA eseguita dovrebbe determinare la scelta da parte del Titolare del trattamento delle misure di protezione dei dati da implementare.

134. È anche importante notare che se i risultati della DPIA indicano che il trattamento comporterebbe rischi elevati nonostante le misure di sicurezza pianificate dal Titolare del trattamento, sarà necessario prima di iniziare il trattamento consultare l'Autorità di controllo competente. I dettagli sui riferimenti precedenti sono inclusi nell'articolo 36.

Per l'European Data Protection Board
Il Presidente
(Andrea Jelinek)