Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video

Versione 2.0

Adottato il 29 gennaio 2020

Storia delle versioni

Versione 2.0	29 gennaio 2020	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	10 luglio 2019	Adozione delle linee guida per la consultazione pubblica

Indice

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, relativo alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE (di seguito "GDPR"),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificato dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

Visti l'articolo 12 e l'articolo 22 del suo regolamento interno,

HA ADOTTATO LE SEGUENTI LINEE GUIDA

1 INTRODUZIONE

1. L'uso intensivo di dispositivi video ha un impatto sul comportamento dei cittadini. Un'implementazione significativa di tali strumenti in molte sfere della vita degli individui eserciterà un'ulteriore pressione sull'individuo per impedire il rilevamento di quelle che potrebbero essere percepite come anomalie. Di fatto, queste tecnologie possono limitare le possibilità di movimento e di utilizzo anonimo dei servizi e, in generale, limitano la possibilità di passare inosservati. Le implicazioni per la protezione dei dati sono enormi.

2. Anche se i singoli individui possono essere a proprio agio con la videosorveglianza impostata per un determinato scopo di sicurezza, ad esempio, è necessario prendere garanzie per evitare qualsiasi uso improprio per scopi completamente diversi e - per l'interessato - inaspettati (ad esempio, scopo di marketing, monitoraggio delle prestazioni dei dipendenti, ecc.) Inoltre, sono stati implementati molti strumenti per sfruttare le immagini acquisite e trasformare le fotocamere tradizionali in fotocamere intelligenti. La quantità di dati generati dal video, combinata con questi strumenti e tecniche, aumenta i rischi di un uso secondario (legato o meno allo scopo originariamente assegnato al sistema) o anche i rischi di un uso improprio. I principi generali del GDPR (articolo 5), dovrebbero sempre essere attentamente considerati quando si tratta di videosorveglianza.

3. I sistemi di videosorveglianza cambiano in molti modi il modo in cui i professionisti del settore privato e pubblico interagiscono in luoghi privati o pubblici allo scopo di migliorare la sicurezza, ottenere un'analisi dell'audience, fornire pubblicità personalizzata, ecc. La videosorveglianza è diventata altamente performante grazie alla crescente implementazione dell'analisi video intelligente. Queste tecniche possono essere più intrusive (ad es. tecnologie biometriche complesse) o meno intrusive (ad es. semplici algoritmi di conteggio). Rimanere anonimi e preservare la propria privacy è in generale sempre più difficile. I problemi di protezione dei dati sollevati in ogni situazione possono differire, così come l'analisi legale quando si utilizza l'una o l'altra di queste tecnologie.

4. Oltre ai problemi di privacy, vi sono anche rischi legati a possibili malfunzionamenti di questi dispositivi e ai pregiudizi che possono indurre. I ricercatori riferiscono che il software utilizzato per l'identificazione facciale, il riconoscimento o l'analisi si comporta in modo diverso in base all'età, al sesso e all'etnia della persona che sta identificando.
   Gli algoritmi si baserebbero su dati demografici diversi, quindi, la parzialità nel riconoscimento

[1] riferimenti agli "Stati membri" fatti nel presente parere vanno intesi come riferimenti agli "Stati membri del SEE".

facciale minaccia di rafforzare i pregiudizi della società. Per questo motivo, i responsabili del trattamento devono anche assicurare che il trattamento dei dati biometrici derivanti dalla videosorveglianza sia sottoposto a una valutazione periodica della sua rilevanza e dell'adeguatezza delle garanzie fornite.

5. La videosorveglianza non è di default una necessità quando ci sono altri mezzi per raggiungere lo scopo sottostante. Altrimenti rischiamo un cambiamento delle norme culturali che porti all'accettazione della mancanza di privacy come inizio generale.

6. Queste linee guida hanno lo scopo di fornire indicazioni su come applicare il GDPR in relazione al trattamento dei dati personali attraverso dispositivi video. Gli esempi non sono esaustivi, il ragionamento generale può essere applicato a tutti i potenziali settori di utilizzo.

2 CAMPO DI APPLICAZIONE[2]

2.1 Dati personali

7. Il monitoraggio sistematico e automatizzato di un determinato spazio con mezzi ottici o audiovisivi, per lo più a scopo di protezione della proprietà, o per proteggere la vita e la salute dell'individuo, è diventato un fenomeno significativo dei nostri giorni. Questa attività comporta la raccolta e la conservazione di informazioni pittoriche o audiovisive su tutte le persone che entrano nello spazio monitorato, identificabili in base al loro aspetto o ad altri elementi specifici. L'identità di queste persone può essere stabilita sulla base di questi dati. Consente inoltre l'ulteriore trattamento dei dati personali per quanto riguarda la presenza e il comportamento delle persone in questo spazio. Il rischio potenziale di un uso improprio di questi dati cresce in relazione alla dimensione dello spazio monitorato e al numero di persone che frequentano lo spazio. Questo fatto è rispecchiato dal regolamento generale sulla protezione dei dati nell'articolo 35, paragrafo 3, lettera c), che impone l'esecuzione di una valutazione d'impatto sulla protezione dei dati in caso di monitoraggio sistematico di uno spazio accessibile al pubblico su vasta scala, nonché nell'articolo 37, paragrafo 1, lettera b), che impone agli incaricati del trattamento di designare un responsabile della protezione dei dati, se il trattamento per sua natura comporta un monitoraggio regolare e sistematico delle persone interessate.

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

> Esempio: Il GDPR non è applicabile per le telecamere finte (cioè qualsiasi telecamera che non funziona come una telecamera e quindi non elabora dati personali). *Tuttavia, in alcuni Stati membri potrebbe essere soggetto ad altre legislazioni.*
>
> Esempio: Le registrazioni da un'altitudine elevata rientrano nel campo di applicazione del GDPR solo se, date le circostanze, i dati elaborati possono essere collegati a una persona specifica.
>
> Esempio: Una videocamera è integrata in un'auto per l'assistenza al parcheggio. Se la telecamera è costruita o regolata in modo tale da non raccogliere informazioni relative a una persona fisica (come le targhe o informazioni che potrebbero identificare i passanti) il GDPR non si applica.

9.

2.2 Applicazione della direttiva sull'applicazione della legge, LED (EU2016/680)

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

2.3 Esenzione per le famiglie

11. Ai sensi dell'articolo 2, paragrafo 2, lettera c), il trattamento di dati personali da parte di una persona fisica nell'ambito di un'attività puramente personale o domestica, che può comprendere anche un'attività online, non rientra nel campo di applicazione del GDPR[3].

12. Questa disposizione - la cosiddetta esenzione domestica - nel contesto della videosorveglianza deve essere interpretata in modo restrittivo. Quindi, come considerato dalla Corte di Giustizia Europea, il cosiddetto "nucleo familiare esenzione" deve "*essere interpretata come relativa solo alle attività che si svolgono nell'ambito della vita privata o familiare delle persone, il che evidentemente non è il caso*

[2] L'IFPDT osserva che, laddove il PILR lo consenta, potrebbero essere applicati requisiti specifici nella legislazione nazionale.

[3] Cfr. anche il considerando 18.

del trattamento di dati personali che consiste nella pubblicazione su internet affinché tali dati siano resi accessibili a un numero indefinito di persone"[4]. Inoltre, se un sistema di videosorveglianza, nella misura in cui comporta la registrazione e la conservazione costante di dati personali e copre, "*anche parzialmente, uno spazio pubblico ed è quindi diretto verso l'esterno dell'ambiente privato della persona che tratta i dati in tal modo, non può essere considerato come un'attività puramente "personale o domestica" ai sensi dell'art. 3, n. 2, secondo trattino, della direttiva 95/46"*[5] .

13. Per quanto riguarda i dispositivi video azionati all'interno dei locali di un privato, possono rientrare nell'esenzione domestica. Dipenderà da diversi fattori, che dovranno essere tutti presi in considerazione per giungere a una conclusione. Oltre agli elementi sopra citati identificati dalle sentenze della Corte di giustizia europea, l'utente della videosorveglianza a casa deve valutare se ha un qualche tipo di rapporto personale con l'interessato, se la portata o la frequenza della sorveglianza suggeriscono un qualche tipo di attività professionale da parte sua, e il potenziale impatto negativo della sorveglianza sui soggetti interessati. La presenza di uno solo dei suddetti elementi non suggerisce necessariamente che il trattamento non rientri nell'ambito di applicazione dell'esenzione per nucleo familiare; per tale determinazione è necessaria una valutazione complessiva.

Esempio: Un turista registra i video sia con il cellulare che con la videocamera per documentare le sue vacanze. Mostra il filmato ad amici e familiari, ma non lo rende accessibile a un numero indefinito di persone. Questo rientrerebbe nell'esenzione per le famiglie.

Esempio: Una mountain biker del downhill vuole registrare la sua discesa con una actioncam. Sta cavalcando in una zona remota e ha intenzione di utilizzare le registrazioni solo per il suo intrattenimento personale a casa. Ciò rientrerebbe nell'esenzione per le famiglie, anche se in una certa misura vengono trattati dati personali.

Esempio: Qualcuno sta monitorando e registrando il suo giardino. La proprietà è recintata e solo il controllore stesso e la sua famiglia entrano regolarmente nel giardino. Ciò rientrerebbe nell'esenzione per le famiglie, a condizione che la videosorveglianza non si estenda anche solo parzialmente a uno spazio pubblico o a una proprietà vicina.

[4] Corte di giustizia europea, sentenza nella causa C-101/01, *causa Bodil Lindqvist*, 6 novembre 2003, paragrafo 47.

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

3 LICEITÀ DEL TRATTAMENTO

15. Prima dell'utilizzo, le finalità del trattamento devono essere specificate in dettaglio (articolo 5, paragrafo 1, lettera b)). La videosorveglianza può servire a molti scopi, ad esempio sostenere la protezione della proprietà e di altri beni, sostenere la protezione della vita e dell'integrità fisica degli individui, raccogliere prove per le cause civili[6] Questi scopi di monitoraggio devono essere documentati per iscritto (articolo 5, paragrafo 2) e devono essere specificati per ogni telecamera di sorveglianza in uso. Le telecamere che vengono utilizzate per lo stesso scopo da un unico controllore possono essere documentate insieme. Inoltre, gli interessati devono essere informati delle finalità del trattamento ai sensi dell'articolo 13 (*cfr. punto 7, Trasparenza e obblighi di informazione*). La videosorveglianza basata sul mero scopo di "sicurezza" o "per la vostra sicurezza" non è sufficientemente specifica (articolo 5, paragrafo 1, lettera b)). È inoltre contrario al principio secondo cui i dati personali devono essere trattati in modo lecito, equo e trasparente nei confronti dell'interessato (cfr. articolo 5, paragrafo 1, lettera a)).

16. In linea di principio, ogni motivo giuridico ai sensi dell'articolo 6, paragrafo 1, può fornire una base giuridica per l'elaborazione dei dati di videosorveglianza. Ad esempio, l'articolo 6, paragrafo 1, lettera c), si applica quando la legislazione nazionale prevede l'obbligo di effettuare la videosorveglianza[7]. Tuttavia, nella pratica, le disposizioni più probabili da utilizzare sono

- Articolo 6, paragrafo 1, lettera f) (interesse legittimo),
- Articolo 6, paragrafo 1, lettera e) (necessità di svolgere un compito di interesse pubblico o nell'esercizio di pubblici poteri).

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

3.1 Interesse legittimo, articolo 6, paragrafo 1, lettera f)

17. La valutazione giuridica dell'articolo 6, paragrafo 1, lettera f), dovrebbe basarsi sui seguenti criteri, conformemente al considerando 47.

3.1.1 Esistenza di interessi legittimi

18. La videosorveglianza è legale se è necessaria per soddisfare lo scopo di un interesse legittimo perseguito da un responsabile del trattamento o da un terzo, a meno che tali interessi non siano superati dagli interessi dell'interessato o dai diritti e dalle libertà fondamentali (articolo 6, paragrafo 1, lettera f)). Gli interessi legittimi perseguiti da un controllore o da un terzo possono essere interessi legali[8], economici o non materiali[9]. Tuttavia, il responsabile del trattamento deve considerare che se l'interessato si oppone alla sorveglianza ai sensi dell'articolo 21, il responsabile del trattamento può procedere alla videosorveglianza dell'interessato solo se si tratta di un interesse legittimo prevalente che prevalga sugli interessi, i diritti e le libertà dell'interessato o per l'accertamento, l'esercizio o la difesa di diritti legali.

19. In una situazione reale e pericolosa, lo scopo di proteggere la proprietà da furti con scasso, furti o atti vandalici può costituire un interesse legittimo per la videosorveglianza.

20. L'interesse legittimo deve essere di esistenza reale e deve essere una questione attuale (cioè non deve essere fittizio o speculativo)[10]. Prima di iniziare la sorveglianza, è necessario che ci sia una

[6] Le norme sulla raccolta delle prove per le cause civili variano da uno Stato membro all'altro.
[7] Le presenti linee guida non analizzano né entrano nei dettagli della legislazione nazionale che potrebbe differire da uno Stato membro all'altro.
[8] Corte di giustizia europea, sentenza nella causa C-13/16, *Rīgas satiksme*, 4 maggio 2017
[9] vedi WP217, Gruppo di lavoro articolo 29
[10] vedi WP217, Gruppo di lavoro articolo 29, pag. 24 e segg. Cfr. anche la sentenza della Corte di giustizia delle Comunità europee nella causa C-708/18, pag. 44.

situazione di pericolo nella vita reale - come ad esempio danni o gravi incidenti in passato - prima di iniziare la sorveglianza. Alla luce del principio di responsabilità, i controllori farebbero bene a documentare gli incidenti rilevanti (data, modalità, perdita finanziaria) e le relative accuse penali. Questi incidenti documentati possono essere una forte prova dell'esistenza di un interesse legittimo. L'esistenza di un interesse legittimo e la necessità del monitoraggio dovrebbero essere rivalutate a intervalli periodici (ad esempio una volta all'anno, a seconda delle circostanze).

Esempio: Il proprietario di un negozio vuole aprire un nuovo negozio e vuole installare un sistema di videosorveglianza per prevenire gli atti vandalici. Egli può dimostrare, presentando le statistiche, che c'è una forte aspettativa di vandalismo nel quartiere vicino. Inoltre, è utile l'esperienza dei negozi vicini. Non è necessario che si sia verificato un danno al regolatore in questione. Finché i danni nel quartiere suggeriscono un pericolo o simili, e quindi possono essere indice di un interesse legittimo. Non è tuttavia sufficiente presentare statistiche nazionali o generali sulla criminalità senza analizzare l'area in questione o i pericoli per questo specifico negozio.

21.

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

23. Il GDPR stabilisce inoltre chiaramente che le autorità pubbliche non possono far valere il loro trattamento per motivi di interesse legittimo, fintantoché svolgono i loro compiti, articolo 6, paragrafo 1, secondo comma.

3.1.2 Necessità di lavorazione

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

25. Data la situazione in cui un controllore vuole prevenire i reati legati alla proprietà, invece di installare un sistema di videosorveglianza, il controllore potrebbe anche adottare misure di sicurezza alternative come la recinzione della proprietà, l'installazione di pattuglie regolari del personale di sicurezza, l'utilizzo di guardiani, la fornitura di una migliore illuminazione, l'installazione di serrature di sicurezza, finestre e porte a prova di manomissione o l'applicazione di rivestimenti anti-graffiti o lamine alle pareti. Queste misure possono essere efficaci quanto i sistemi di videosorveglianza contro i furti con scasso, i furti e gli atti vandalici. Il controllore deve valutare caso per caso se tali misure possono essere una soluzione ragionevole.

26. Prima di mettere in funzione un sistema di telecamere, il controllore è tenuto a valutare dove e quando le misure di videosorveglianza sono strettamente necessarie. Di solito un sistema di sorveglianza funzionante sia di notte che al di fuori del normale orario di lavoro soddisfa le esigenze del controllore per prevenire eventuali pericoli per la sua proprietà.

27. In generale, la necessità di utilizzare la videosorveglianza per proteggere i locali dei controllori termina ai confini della proprietà[11]. Tuttavia, vi sono casi in cui la sorveglianza della proprietà non è sufficiente per una protezione efficace. In alcuni casi individuali potrebbe essere necessario superare la videosorveglianza nelle immediate vicinanze dei locali. In questo contesto, il controllore dovrebbe considerare mezzi fisici e tecnici, ad esempio il blocco o il pixelating di aree non rilevanti.

Esempio: Una libreria vuole proteggere i suoi locali dal vandalismo. In generale, le telecamere dovrebbero filmare i locali stessi solo perché non è necessario guardare i locali vicini o le aree pubbliche nei dintorni dei locali della libreria a tale scopo.

28.

29. Si pone inoltre la questione della necessità del trattamento anche per quanto riguarda le modalità di conservazione delle prove. In alcuni casi potrebbe essere necessario utilizzare soluzioni di scatola nera in cui le riprese vengono automaticamente cancellate dopo un certo periodo di conservazione e accessibili solo in caso di incidente. In altre situazioni, potrebbe non essere necessario registrare il materiale video, ma è più appropriato utilizzare il monitoraggio in tempo reale. Anche la decisione tra soluzioni con scatola nera e monitoraggio in tempo reale dovrebbe essere basata sullo scopo perseguito. Se ad esempio lo scopo della videosorveglianza è la conservazione delle prove, i metodi in tempo reale di solito non sono adatti. A volte il monitoraggio in tempo reale può anche essere più intrusivo rispetto alla memorizzazione e alla cancellazione automatica del materiale dopo un periodo di tempo limitato (ad esempio, se qualcuno visualizza costantemente il monitor, potrebbe essere più intrusivo che se non c'è nessun monitor e il materiale viene memorizzato direttamente in una scatola nera). In questo contesto va considerato il principio della minimizzazione dei dati (articolo 5, paragrafo 1, lettera c)). Va inoltre tenuto presente che potrebbe essere possibile che il controllore si avvalga di personale di sicurezza al posto della videosorveglianza in grado di reagire e di intervenire immediatamente.

3.1.3 Bilanciamento degli interessi

30. Presumendo che la videosorveglianza sia necessaria per proteggere gli interessi legittimi di un responsabile del trattamento, un sistema di videosorveglianza può essere messo in funzione solo se gli interessi legittimi del responsabile del trattamento o quelli di terzi (ad esempio la protezione della proprietà o dell'integrità fisica) non sono superati dagli interessi o dai diritti e dalle libertà fondamentali dell'interessato. Il responsabile del trattamento deve considerare 1) in che misura il controllo incide sugli interessi, i diritti e le libertà fondamentali delle persone e 2) se ciò provoca violazioni o conseguenze negative per quanto riguarda i diritti dell'interessato. In effetti,
Il bilanciamento degli interessi è obbligatorio. I diritti e le libertà fondamentali, da un lato, e i legittimi interessi del controllore, dall'altro, devono essere valutati ed equilibrati con attenzione.

Esempio: Una società di parcheggi privati ha documentato problemi ricorrenti di furti nelle auto parcheggiate. Il parcheggio è uno spazio aperto e facilmente accessibile a chiunque, ma è chiaramente segnalato con cartelli e blocchi stradali che circondano lo spazio. La società di parcheggio ha un interesse legittimo (prevenire i furti nelle auto dei clienti) a monitorare l'area durante l'ora del giorno in cui si verificano problemi. Gli interessati sono monitorati in un periodo di tempo limitato, non si trovano nella zona a scopo ricreativo ed è anche nel loro stesso interesse che i furti siano evitati. L'interesse degli interessati a non essere monitorati è in questo caso prevalso sull'interesse legittimo del titolare del trattamento.

Esempio: Un ristorante decide di installare videocamere nei bagni per controllare l'ordine dei servizi igienici. In questo caso i diritti degli interessati prevalgono chiaramente sull'interesse del titolare del trattamento, pertanto non è possibile installare telecamere.

3.1.3.1 Prendere decisioni caso per caso

32. Poiché la ponderazione degli interessi è obbligatoria ai sensi del regolamento, la decisione deve essere presa caso per caso (cfr. articolo 6, paragrafo 1, lettera f)). Non è sufficiente fare riferimento a situazioni astratte o confrontare tra loro casi simili. Il responsabile del trattamento deve valutare i

[11] Anche questo potrebbe essere soggetto alla legislazione nazionale in alcuni Stati membri.

rischi di intrusione nei diritti dell'interessato; qui il criterio decisivo è l'intensità dell'intervento per i diritti e le libertà dell'individuo.

33. L'intensità può essere definita, tra l'altro, in base al tipo di informazioni raccolte (contenuto dell'informazione), alla portata (densità dell'informazione, estensione spaziale e geografica), al numero di persone interessate, sia come numero specifico che come percentuale della popolazione interessata, alla situazione in questione, agli interessi reali del gruppo di persone interessate, ai mezzi alternativi, nonché alla natura e alla portata della valutazione dei dati.

34. Importanti fattori di bilanciamento possono essere le dimensioni dell'area, che è sotto sorveglianza, e la quantità di soggetti sotto sorveglianza. L'uso della videosorveglianza in un'area remota (ad esempio per osservare la fauna selvatica o per proteggere infrastrutture critiche come un'antenna radio privata) deve essere valutato in modo diverso rispetto alla videosorveglianza in una zona pedonale o in un centro commerciale.

Esempio: Se viene installata una telecamera sul cruscotto (ad esempio per accogliere le prove in caso di incidente), è importante assicurarsi che questa telecamera non registri costantemente il traffico, così come le persone che si trovano in prossimità di una 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 degli interessati.

35.

3.1.3.2 Le ragionevoli aspettative degli interessati

36. 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, il rapporto tra l'interessato e il responsabile del trattamento può variare in modo significativo e può influire sulle ragionevoli aspettative dell'interessato. L'interpretazione del concetto di aspettative ragionevoli non dovrebbe basarsi solo sulle aspettative soggettive in questione. Il criterio decisivo deve piuttosto essere il fatto che un terzo obiettivo possa ragionevolmente aspettarsi e concludere di essere soggetto a monitoraggio in questa specifica situazione.

37. Ad esempio, nella maggior parte dei casi un dipendente sul posto di lavoro non si aspetta di essere monitorato dal suo datore di lavoro[12]. Inoltre, il monitoraggio non è previsto nel giardino privato, negli spazi abitativi o nelle sale per esami e trattamenti. Allo stesso modo, non è ragionevole aspettarsi un monitoraggio negli impianti sanitari o nelle saune - il monitoraggio di tali aree è un'intensa intrusione nei diritti della persona interessata. La ragionevole aspettativa degli interessati è che non si verifichi alcuna videosorveglianza in quelle aree. D'altra parte, il cliente di una banca potrebbe aspettarsi di essere monitorato all'interno della banca o dal bancomat.

38. Gli interessati possono anche aspettarsi di essere liberi di essere monitorati all'interno di aree accessibili al pubblico, soprattutto se tali aree sono tipicamente utilizzate per il recupero, la rigenerazione e le attività del tempo libero, nonché in luoghi in cui gli individui soggiornano e/o comunicano, come aree di seduta, tavoli in ristoranti, parchi, cinema e strutture per il fitness. In questo caso gli interessi o i diritti e le libertà dell'interessato prevalgono spesso sugli interessi legittimi del responsabile del trattamento.

Esempio: Nei servizi igienici gli interessati non si aspettano di essere monitorati. La videosorveglianza, ad esempio per prevenire gli incidenti, non è proporzionale.

39.

40. I segnali che informano l'interessato sulla videosorveglianza non hanno alcuna rilevanza nel

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

determinare ciò che un interessato può oggettivamente aspettarsi. Ciò significa che, ad esempio, il proprietario di un negozio non può fare affidamento sul fatto che i clienti abbiano *oggettivamente* ragionevoli aspettative di essere sorvegliati solo perché un cartello informa la persona all'ingresso della sorveglianza.

3.2 Necessità di svolgere un compito di interesse pubblico o nell'esercizio dei pubblici poteri di cui è investito il responsabile del trattamento, articolo 6, paragrafo 1, lettera e)

41. I dati personali possono essere trattati mediante la videosorveglianza di cui all'articolo 6, paragrafo 1, lettera e), se necessario per l'espletamento di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri[13]. Può darsi che l'esercizio dei pubblici poteri non consenta tale trattamento, ma altre basi legislative, come "salute e sicurezza" per la tutela dei visitatori e dei dipendenti, possono prevedere un margine di manovra limitato per il trattamento, sempre nel rispetto degli obblighi GDPR e dei diritti degli interessati.

42. Gli Stati membri possono mantenere o introdurre una legislazione nazionale specifica in materia di videosorveglianza per adattare l'applicazione delle norme del GDPR, determinando con maggiore precisione i requisiti specifici per il trattamento, purché sia conforme ai principi stabiliti dal GDPR (ad esempio, limitazione della conservazione, proporzionalità).

[13] Le basi del trattamento in questione sono stabilite dal diritto dell'Unione o dal diritto degli Stati membri" e "sono necessarie per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il responsabile del trattamento (articolo 6, paragrafo 3).

3.3 Consenso, articolo 6, paragrafo 1, lettera a)

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

44. Per quanto riguarda il controllo sistematico, il consenso della persona interessata può fungere da base giuridica ai sensi dell'articolo 7 (cfr. considerando 43) solo in casi eccezionali. È nella natura della sorveglianza che questa tecnologia monitora un numero imprecisato di persone contemporaneamente. Il responsabile del trattamento difficilmente potrà dimostrare che l'interessato ha dato il suo consenso prima del trattamento dei suoi dati personali (articolo 7, paragrafo 1). Supponendo che l'interessato revochi il proprio consenso, sarà difficile per il responsabile del trattamento dimostrare che i dati personali non sono più oggetto di trattamento.

45.

> Esempio: Gli atleti possono richiedere il monitoraggio durante gli esercizi individuali per analizzare le loro tecniche e le loro prestazioni. D'altra parte, quando una società sportiva prende l'iniziativa di monitorare un'intera squadra per lo stesso scopo, il consenso spesso non sarà valido, in quanto i singoli atleti possono sentirsi spinti a dare il consenso in modo che il loro rifiuto non influisca negativamente sui compagni di squadra.

46. Se il responsabile del trattamento desidera fare affidamento sul consenso, è suo dovere assicurarsi che ogni soggetto interessato che entra nell'area sottoposta a videosorveglianza abbia dato il proprio consenso. Tale consenso deve soddisfare le condizioni di cui all'articolo 7. L'ingresso in un'area monitorata contrassegnata (ad esempio, le persone sono invitate a passare attraverso un corridoio o un cancello specifico per entrare in un'area monitorata) non costituisce una dichiarazione o una chiara azione positiva necessaria per il consenso, a meno che non soddisfi i criteri dell'articolo 4 e 7, come descritto nelle linee guida sul consenso[15].

47. 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 per il trattamento dei dati personali, in quanto è improbabile che venga dato liberamente. Le linee guida sul consenso dovrebbero essere prese in considerazione in questo contesto.

48. La legge dello Stato membro o i contratti collettivi, compresi i "contratti di lavoro", possono prevedere norme specifiche sul trattamento dei dati personali dei dipendenti nel contesto dell'occupazione (cfr. articolo 88).

[14] Gruppo di lavoro dell'articolo 29 (art. 29 WP) "Linee guida per il consenso ai sensi del regolamento 2016/679" (WP 259 rev. 01). - approvato dall'EDPB

[15] Gruppo di lavoro articolo 29 (art. 29 WP) "Linee guida sul consenso ai sensi del regolamento 2016/679" (WP 259) - approvate dall'IFPD - di cui occorre tenere conto.

4 LA DIVULGAZIONE DI FILMATI VIDEO A TERZI

49. In linea di principio, le norme generali del GDPR si applicano alla divulgazione di registrazioni video a terzi.

4.1 Divulgazione di filmati a terzi in generale

50. Per divulgazione si intende la trasmissione (ad es. comunicazione individuale), la diffusione (ad es. pubblicazione online) o la messa a disposizione in altro modo. I terzi sono definiti all'articolo 4, paragrafo 10. In caso di divulgazione a paesi terzi o organizzazioni internazionali, si applicano anche le disposizioni speciali dell'articolo 44 e seguenti.

51. L'eventuale comunicazione di dati personali costituisce un tipo di trattamento distinto di dati personali per il quale il responsabile del trattamento deve avere una base giuridica nell'articolo 6.

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

52

53. La trasmissione di filmati video a terzi per scopi diversi da quello per cui sono stati raccolti i dati è possibile ai sensi dell'articolo 6, paragrafo 4.

> Esempio: La videosorveglianza di una barriera (in un parcheggio) è installata allo scopo di risolvere i danni. Si verifica un danno e la registrazione viene trasferita ad un avvocato per portare avanti il caso. In questo caso lo scopo della registrazione è lo stesso di quello del trasferimento.
>
> Esempio: La videosorveglianza di una barriera (in un parcheggio) è installata allo scopo di risolvere i danni. La registrazione viene pubblicata online per puro divertimento. In questo caso lo scopo è cambiato e non è compatibile con lo scopo iniziale. Sarebbe inoltre problematico individuare una base giuridica per tale elaborazione (pubblicazione).

54.

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

4.2 Divulgazione di filmati alle forze dell'ordine

56. Anche la divulgazione delle registrazioni video alle forze dell'ordine è un processo indipendente, che richiede una giustificazione separata per il controllore.

57. Ai sensi dell'articolo 6, paragrafo 1, lettera c), il trattamento è legale se è necessario per l'adempimento di un obbligo legale al quale è soggetto il responsabile del trattamento. Sebbene il diritto di polizia applicabile sia un affare sotto il controllo esclusivo degli Stati membri, esistono molto probabilmente norme generali che regolano il trasferimento delle prove alle forze dell'ordine in ogni Stato membro. Il trattamento dei dati da parte del responsabile del trattamento è regolato dal GDPR. Se la legislazione nazionale impone al responsabile del trattamento di cooperare con le forze dell'ordine (ad es. indagini), la base giuridica per la trasmissione dei dati è l'obbligo giuridico di cui all'articolo 6, paragrafo 1, lettera c).

58. La limitazione delle finalità di cui all'articolo 6, paragrafo 4, non è quindi spesso problematica, poiché la divulgazione risale esplicitamente alla legislazione degli Stati membri. Una considerazione dei requisiti speciali per un cambiamento di destinazione nel senso della lettera a - e non è quindi necessaria.

Esempio: Il proprietario di un negozio registra i filmati all'ingresso. Il filmato mostra una persona che ruba il portafoglio di un'altra persona. La polizia chiede al controllore di consegnare il materiale per aiutarla nelle indagini. In tal caso, il titolare del negozio utilizzerebbe la base giuridica di cui all'articolo 6, paragrafo 1, lettera c) (obbligo giuridico) in combinato disposto con la legge nazionale pertinente per l'elaborazione del trasferimento.

59.

Esempio: Una telecamera viene installata in un negozio per motivi di sicurezza. Il proprietario del negozio crede di aver registrato qualcosa di sospetto nel suo filmato e decide di inviare il materiale alla polizia (senza alcuna indicazione che ci sia un'indagine in corso di qualche tipo). In questo caso il titolare del negozio deve valutare se le condizioni di cui, nella maggior parte dei casi, all'articolo 6, paragrafo 1, lettera f), sono soddisfatte. Questo avviene di solito se il proprietario del negozio ha il ragionevole sospetto che sia stato commesso un reato.

60.

61. Il trattamento dei dati personali da parte delle stesse forze dell'ordine non segue il GDPR (cfr. articolo 2, paragrafo 2, lettera d)), ma segue invece la direttiva sulle forze dell'ordine (EU2016/680).

5 TRATTAMENTO DI PARTICOLARI CATEGORIE DI DATI

62. I sistemi di videosorveglianza raccolgono di solito quantità massicce di dati personali che possono rivelare dati di natura altamente personale e anche categorie particolari di dati. In effetti, dati apparentemente non significativi originariamente raccolti attraverso il video possono essere utilizzati per dedurre altre informazioni per raggiungere uno scopo diverso (ad esempio, per mappare le abitudini di un individuo). Tuttavia, la videosorveglianza non è sempre considerata come trattamento di particolari categorie di dati personali.

63.

Esempio: I filmati che mostrano un soggetto che indossa occhiali o usa una sedia a rotelle non sono di per sé considerati come categorie speciali di dati personali.

64. Tuttavia, se le riprese video vengono elaborate per dedurre particolari categorie di dati si applica l'articolo 9.

65.

Esempio: Le opinioni politiche possono essere dedotte, ad esempio, da immagini che mostrano oggetti identificabili che partecipano a un evento, partecipano a uno sciopero, ecc. Ciò rientrerebbe nell'articolo 9.

Esempio: Un ospedale che installa una videocamera per monitorare lo stato di salute di un paziente sarebbe considerato come trattamento di particolari categorie di dati personali

66. In generale, in linea di principio, ogni volta che si installa un sistema di videosorveglianza si dovrebbe considerare attentamente il principio della minimizzazione dei dati. Pertanto, anche nei casi in cui non si applica l'articolo 9, paragrafo 1, il responsabile del trattamento dovrebbe sempre cercare di ridurre al minimo il rischio di catturare filmati che rivelino altri dati sensibili (oltre all'articolo 9), indipendentemente dalla finalità.

67.

Esempio: La videosorveglianza che cattura una chiesa non rientra di per sé nell'articolo 9.
Tuttavia, il responsabile del trattamento deve effettuare una valutazione particolarmente attenta ai sensi dell'articolo 6, paragrafo 1, lettera f), tenendo conto della natura dei dati nonché del rischio di acquisire altri dati sensibili (oltre all'articolo 9) nel valutare gli interessi dell'interessato.

68. Se per il trattamento di categorie particolari di dati viene utilizzato un sistema di videosorveglianza, il responsabile del trattamento deve individuare sia un'eccezione per il trattamento di categorie particolari di dati ai sensi dell'articolo 9 (ossia un'esenzione dalla regola generale secondo cui non si devono trattare categorie particolari di dati), sia una base giuridica ai sensi dell'articolo 6.

69. Ad esempio, l'articolo 9, paragrafo 2, lettera c) ("[...] *il trattamento è necessario per tutelare gli interessi vitali dell'interessato o di un'altra persona fisica* [...]") potrebbe - in teoria e in via eccezionale - essere utilizzato, ma il responsabile del trattamento dovrebbe giustificarlo come una necessità assoluta per salvaguardare gli interessi vitali di una persona e dimostrare che tale "[...] interessato è *fisicamente o giuridicamente incapace di dare il proprio consenso".* Inoltre, il titolare del trattamento non potrà utilizzare il sistema per nessun altro motivo.

70. È importante notare in questa sede che ogni esenzione elencata all'art. 9 non può essere utilizzata per giustificare il trattamento di particolari categorie di dati attraverso la videosorveglianza. In particolare, i responsabili del trattamento di tali dati nell'ambito della videosorveglianza non possono invocare l'art. 9, paragrafo 2, lettera e), che consente il trattamento di dati personali manifestamente resi pubblici dall'interessato. Il semplice fatto di entrare nel raggio d'azione della telecamera non implica che l'interessato intenda rendere pubbliche particolari categorie di dati che lo riguardano.

71. Inoltre, il trattamento di categorie speciali di dati richiede una maggiore e costante vigilanza su determinati obblighi; ad esempio, un elevato livello di sicurezza e una valutazione d'impatto sulla protezione dei dati, se necessario.

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

72.

5.1 Considerazioni generali nell'elaborazione dei dati biometrici

73. L'utilizzo di dati biometrici e in particolare il riconoscimento facciale comportano rischi maggiori per i diritti delle persone interessate. È fondamentale che il ricorso a tali tecnologie avvenga nel rispetto dei principi di legalità, necessità, proporzionalità e minimizzazione dei dati, come stabilito dal GDPR. Mentre l'uso di queste tecnologie può essere percepito come particolarmente efficace, i responsabili del trattamento dovrebbero prima di tutto valutare l'impatto sui diritti e sulle libertà fondamentali e considerare mezzi meno invasivi per raggiungere il loro legittimo scopo del trattamento.

74. Per qualificarsi come dati biometrici secondo la definizione del GDPR, l'elaborazione di dati grezzi, 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 nel suo articolo 4.14 che è "*[...] risultante da specifiche elaborazioni tecniche relative alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che consentono o confermano l'identificazione univoca di tale persona fisica [...]".* Le riprese video di una persona non possono tuttavia essere considerate di per sé come dati biometrici ai sensi dell'articolo 9, se non sono state specificamente elaborate tecnicamente per contribuire all'identificazione di una persona[16].

75. Affinché possa essere considerato un trattamento di particolari categorie di dati personali (articolo 9) è necessario che i dati biometrici siano trattati "al fine di identificare in modo univoco una persona fisica".

76. Riassumendo, alla luce dell'articolo 4.14 e 9, si devono considerare tre criteri:

- **Natura dei dati:** dati relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica,
- **Mezzi e modalità di elaborazione**: dati "risultanti da un'elaborazione tecnica specifica",
- **Scopo del trattamento:** i dati devono essere utilizzati per identificare in modo univoco una persona fisica.

77. L'uso della videosorveglianza, inclusa la funzionalità di riconoscimento biometrico, installata da soggetti privati per i propri scopi (ad es. marketing, statistica o anche sicurezza) richiederà, nella maggior parte dei casi, il consenso esplicito di tutti gli interessati (articolo 9, paragrafo 2, lettera a)), ma potrebbe essere applicabile anche un'altra idonea eccezione all'articolo 9.

[16] Il considerando 51 del GDPR sostiene questa analisi, affermando che "*[...] Il trattamento di fotografie non dovrebbe essere sistematicamente considerato come un trattamento di categorie particolari di dati personali, in quanto rientrano nella definizione di dati biometrici solo quando sono trattati attraverso un mezzo tecnico specifico che consente l'identificazione o l'autenticazione unica di una persona fisica. […]*".

Esempio: Per migliorare il proprio servizio una compagnia privata sostituisce i punti di controllo per l'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 avranno precedentemente dato il loro consenso esplicito e informato, dovranno arruolarsi ad esempio in 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, ad esempio il sistema deve essere installato all'interno di un portale, in modo che i modelli biometrici delle persone non consenzienti non vengano rilevati. Solo i passeggeri, che avranno preventivamente dato il loro consenso e procederanno all'iscrizione, utilizzeranno il portale dotato di sistema biometrico.

Esempio: Un controllore gestisce l'accesso al suo edificio utilizzando un metodo di riconoscimento facciale. Le persone possono utilizzare questa modalità di accesso solo se hanno dato il loro consenso esplicitamente informato (ai sensi dell'articolo 9, paragrafo 2, lettera a))) in anticipo. Tuttavia, per garantire che non venga catturato nessuno che non abbia precedentemente dato il proprio consenso, il metodo di riconoscimento facciale dovrebbe essere attivato dall'interessato stesso, ad esempio premendo un pulsante. Per garantire la liceità del trattamento, il responsabile del trattamento deve sempre offrire una modalità

78.

79. In questo tipo di casi, in cui vengono generati modelli biometrici, i responsabili del trattamento provvedono affinché, una volta ottenuto un risultato di match o no-match, tutti i modelli intermedi realizzati al volo (con il consenso esplicito e informato dell'interessato) per essere confrontati con quelli creati dall'interessato al momento dell'arruolamento, vengano immediatamente e in modo sicuro cancellati. I modelli creati per l'arruolamento devono essere conservati solo per la realizzazione dello scopo dell'elaborazione e non devono essere memorizzati o archiviati.

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

Esempio: Il proprietario di un negozio vorrebbe personalizzare la sua pubblicità in base alle caratteristiche di genere e di età del cliente catturate da un sistema di videosorveglianza. Se tale sistema non genera modelli biometrici per identificare in modo univoco le persone, ma si limita a rilevare tali caratteristiche fisiche per classificare la persona, il trattamento non rientra nel campo di applicazione dell'articolo 9 (purché non vengano trattati altri tipi di categorie speciali di dati).

81.

82. Tuttavia, l'articolo 9 si applica se il responsabile del trattamento memorizza dati biometrici (più comunemente attraverso modelli creati mediante l'estrazione di caratteristiche chiave dalla forma grezza dei dati biometrici (ad es. misurazioni facciali da un'immagine)) al fine di identificare in modo univoco una persona. Se un responsabile del trattamento desiderasse rilevare un soggetto che rientra nell'area o che entra in un'altra area (ad esempio per proiettare un annuncio pubblicitario personalizzato), lo scopo sarebbe quello di identificare in modo univoco una persona fisica, il che significa che l'operazione rientrerebbe fin dall'inizio nell'ambito di applicazione dell'articolo 9. Questo potrebbe essere il caso se un controllore memorizza i modelli generati per fornire ulteriore pubblicità su misura su più cartelloni pubblicitari in diversi punti all'interno del negozio. Poiché il sistema utilizza caratteristiche fisiche per rilevare specifici individui che rientrano nel raggio d'azione della telecamera (come i visitatori di un centro commerciale) e per tracciarli, costituirebbe un metodo di identificazione biometrica perché finalizzato al riconoscimento attraverso l'uso di specifiche elaborazioni tecniche.

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

83.

84. L'EDPB osserva che alcuni sistemi biometrici sono installati in ambienti non controllati[17], il che significa che il sistema prevede la cattura al volo dei volti di qualsiasi individuo che passa nel raggio d'azione della telecamera, comprese le persone che non hanno acconsentito al dispositivo biometrico, e quindi la creazione di modelli biometrici. Questi modelli vengono confrontati con quelli creati da persone che hanno dato il loro previo consenso durante un processo di arruolamento (cioè un utente biometrico) affinché il responsabile del trattamento dei dati riconosca se la persona è un utente di dispositivi biometrici o meno. In questo caso, il sistema è spesso progettato per discriminare gli individui che vuole riconoscere da un database da quelli che non sono arruolati. Poiché lo scopo è quello di identificare in modo univoco le persone fisiche, è ancora necessaria un'eccezione ai sensi dell'articolo 9, paragrafo 2 del GDPR per chiunque venga ripreso dalla telecamera.

Esempio: Un hotel utilizza la videosorveglianza per avvisare automaticamente il gestore dell'hotel che un VIP è arrivato quando il volto dell'ospite viene riconosciuto. Questi VIP hanno dato il loro esplicito consenso all'uso del riconoscimento facciale prima di essere registrati in una banca dati creata 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) non abbiano acconsentito al trattamento ai sensi dell'articolo 9, paragrafo 2, lettera a) del GDPR.

Esempio: Un controllore installa un sistema di videosorveglianza con riconoscimento facciale all'ingresso della sala da concerto da lui gestita. Il controllore deve impostare ingressi chiaramente separati; uno con un sistema biometrico e uno senza (dove invece si scansiona ad esempio un biglietto). Gli ingressi dotati di dispositivi biometrici, devono essere installati e resi accessibili in modo da evitare che il sistema catturi modelli biometrici di spettatori non

85.

86. Infine, quando il consenso è richiesto dall'articolo 9 GDPR, il responsabile del trattamento non condiziona l'accesso ai suoi servizi all'accettazione del trattamento biometrico. In altre parole, in particolare quando il trattamento biometrico viene utilizzato a scopo di autenticazione, il responsabile del trattamento deve offrire una soluzione alternativa che non comporti un trattamento biometrico - senza restrizioni o costi aggiuntivi per la persona interessata. Questa soluzione alternativa è necessaria anche per le persone che non rispettano i vincoli del dispositivo biometrico (iscrizione o lettura dei dati biometrici impossibile, situazione di disabilità che ne rende difficile l'utilizzo, ecc.) e in previsione di una indisponibilità del dispositivo biometrico (come un malfunzionamento del dispositivo), deve essere implementata una "soluzione di back-up" per garantire la continuità del servizio proposto, limitata però ad un uso eccezionale. In casi eccezionali, può verificarsi una situazione in cui il trattamento dei dati biometrici è l'attività principale di un servizio fornito per contratto, ad es. museo che allestisce una mostra per dimostrare l'uso di un dispositivo di riconoscimento facciale, nel qual caso l'interessato non potrà rifiutare l'elaborazione dei dati biometrici se desidera partecipare alla mostra. In tal caso il consenso richiesto dall'articolo 9 è

[17] Significa che il dispositivo biometrico si trova in uno spazio aperto al pubblico ed è in grado di lavorare su chiunque passi, a differenza dei sistemi biometrici in ambienti controllati che possono essere utilizzati solo da partecipazione della persona consenziente.

ancora valido se sono soddisfatti i requisiti di cui all'articolo 7.

5.2 Misure suggerite per ridurre al minimo i rischi nel trattamento dei dati5.2 biometrici

87. In conformità al principio di minimizzazione dei dati, i responsabili del trattamento devono garantire che i dati estratti da un'immagine digitale per costruire un modello non siano eccessivi e contengano solo le informazioni necessarie per lo scopo specificato, evitando così ogni possibile ulteriore elaborazione. Si dovrebbero adottare misure per garantire che i modelli non possano essere trasferiti attraverso i sistemi biometrici.

88. L'identificazione e l'autenticazione/conversione richiederanno probabilmente la memorizzazione del modello per un successivo confronto. Il responsabile del trattamento dei dati deve considerare il luogo più appropriato per la memorizzazione dei dati. In un ambiente sotto controllo (corridoi delimitati o checkpoint), i template devono essere memorizzati su un singolo dispositivo tenuto dall'utente e sotto il suo unico controllo (in uno smartphone o nella carta d'identità) o - quando necessario per scopi specifici e in presenza di esigenze oggettive - memorizzati in un database centralizzato in forma criptata con una chiave/segreta nelle sole mani della persona per impedire l'accesso non autorizzato al template o al luogo di memorizzazione. Se il responsabile del trattamento dei dati non può evitare di accedere ai modelli, deve adottare le misure appropriate per garantire la sicurezza dei dati memorizzati. Ciò può includere la crittografia del modello utilizzando un algoritmo crittografico.

89. In ogni caso, il responsabile del trattamento adotta tutte le precauzioni necessarie per preservare la disponibilità, l'integrità e la riservatezza dei dati trattati. A tal fine, il responsabile del trattamento adotta in particolare le seguenti misure: compartimentare i dati durante la trasmissione e la memorizzazione, memorizzare i modelli biometrici e i dati grezzi o i dati di identità su database distinti, cifrare i dati biometrici, in particolare i modelli biometrici, e definire una politica di cifratura e di gestione delle chiavi, integrare una misura organizzativa e tecnica per l'individuazione delle frodi, associare un codice di integrità ai dati (ad esempio firma o hash) e vietare qualsiasi accesso esterno ai dati biometrici. Tali misure dovranno evolvere con il progresso delle tecnologie.

90. Inoltre, i responsabili del trattamento dei dati dovrebbero procedere alla cancellazione dei dati grezzi (immagini del volto, segnali vocali, andatura, ecc.) e garantire l'efficacia di questa cancellazione. Se non esiste più una base legale per l'elaborazione, i dati grezzi devono essere cancellati. Infatti, nella misura in cui i template biometrici derivano da tali dati, si può considerare che la costituzione di database potrebbe rappresentare una minaccia uguale se non addirittura maggiore (perché può non essere sempre facile leggere un template biometrico senza la conoscenza di come è stato programmato, mentre i dati grezzi saranno i mattoni di qualsiasi template). Nel caso in cui il responsabile del trattamento debba conservare tali dati, devono essere esplorati i metodi antidisturbo (come il watermarking), che renderebbero inefficace la creazione del template. Il controllore deve inoltre cancellare i dati biometrici e i modelli in caso di accesso non autorizzato al terminale di lettura-comparazione o al server di memorizzazione e cancellare tutti i dati non utili per l'ulteriore elaborazione al termine della vita del dispositivo biometrico.

6 DIRITTI DELL'INTERESSATO

91. A causa del carattere dell'elaborazione dei dati nell'uso della videosorveglianza, alcuni diritti delle persone interessate ai sensi del GDPR servono ulteriori chiarimenti. Questo capitolo non è tuttavia esaustivo, tutti i diritti previsti dal GDPR si applicano al trattamento dei dati personali attraverso la videosorveglianza.

6.1 Diritto di accesso

92. L'interessato ha diritto di ottenere dal titolare del trattamento la conferma dell'esistenza o meno di propri dati personali. Per la videosorveglianza ciò significa che se nessun dato viene memorizzato o trasferito in alcun modo, una volta trascorso il momento di monitoraggio in tempo reale, il titolare del trattamento può solo dare l'informazione che nessun dato personale è più oggetto di trattamento (oltre agli obblighi generali di informazione di cui all'articolo 13, si veda il *paragrafo 7 - Trasparenza e obblighi di informazione*). Se tuttavia i dati sono ancora in corso di trattamento al momento della richiesta (cioè se i dati sono memorizzati o trattati in modo continuativo in qualsiasi altro modo), l'interessato deve ricevere accesso e informazioni ai sensi dell'articolo 15.

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

- Articolo 15, paragrafo 4 del PILR, pregiudica i diritti altrui

94. Dato che un numero qualsiasi di soggetti interessati può essere registrato nella stessa sequenza di videosorveglianza, una proiezione provocherebbe un ulteriore trattamento dei dati personali di altri soggetti. Se l'interessato desidera ricevere una copia del materiale (articolo 15, paragrafo 3), ciò potrebbe pregiudicare i diritti e le libertà degli altri interessati. Per evitare tale effetto il responsabile del trattamento deve pertanto tenere conto del fatto che, a causa della natura intrusiva dei filmati, in alcuni casi il responsabile del trattamento non deve distribuire filmati in cui siano identificabili altri soggetti. La tutela dei diritti di terzi non deve tuttavia essere utilizzata come pretesto per impedire legittime rivendicazioni di accesso da parte di persone fisiche; in questi casi il responsabile del trattamento deve attuare misure tecniche per soddisfare la richiesta di accesso (ad esempio, la modifica delle immagini come il mascheramento o lo scrambling).

- Articolo 11 (2) GDPR, il responsabile del trattamento non è in grado di identificare l'interessato

95. Se il filmato non è ricercabile per i dati personali, (cioè il responsabile del trattamento dovrebbe probabilmente passare attraverso una grande quantità di materiale memorizzato per trovare l'interessato in questione) il responsabile del trattamento potrebbe non essere in grado di identificare l'interessato.

96. Per tali ragioni l'interessato dovrebbe (oltre ad identificarsi anche con documento di identità o di persona) nella sua richiesta al responsabile del trattamento, specificare quando - entro un ragionevole lasso di tempo in proporzione alla quantità di dati registrati - è entrato nell'area monitorata. Il responsabile del trattamento deve comunicare preventivamente all'interessato le informazioni necessarie affinché il responsabile del trattamento possa soddisfare la richiesta. Se il responsabile del trattamento è in grado di dimostrare di non essere in grado di identificare l'interessato, il responsabile del trattamento deve informare l'interessato di conseguenza, se possibile. In tale situazione, nella sua risposta all'interessato, il responsabile del trattamento deve informare l'interessato sull'area esatta per il monitoraggio, la verifica delle telecamere che erano in uso, ecc. in modo che l'interessato abbia la piena comprensione di quali dati personali possono essere stati trattati.

Esempio: Se un interessato richiede una copia dei suoi dati personali trattati attraverso la videosorveglianza all'ingresso di un centro commerciale con 30.000 visitatori al giorno, l'interessato deve specificare quando ha superato l'area monitorata entro circa un'ora. Se il controllore elabora ancora il materiale, deve essere fornita una copia del filmato video. Se altri soggetti possono essere identificati nello stesso materiale, allora quella parte del materiale deve essere resa anonima (ad esempio, sfocando la copia o parti di essa) prima di consegnare la copia all'interessato che ha presentato la richiesta.

Esempio: Se il responsabile del trattamento cancella automaticamente tutti i filmati, ad esempio entro 2 giorni, il responsabile del trattamento non è in grado di fornire i filmati all'interessato dopo questi 2 giorni. Se il responsabile del trattamento riceve una richiesta dopo questi 2 giorni, l'interessato deve esserne informato.

97.

- Articolo 12 PILR, richieste eccessive

98. In caso di richieste eccessive o manifestamente infondate da parte dell'interessato, il responsabile del trattamento può esigere un compenso ragionevole ai sensi dell'articolo 12, paragrafo 5, lettera a), GDPR, oppure rifiutare di dare seguito alla richiesta (articolo 12, paragrafo 5, lettera b), GDPR). Il controllore deve essere in grado di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

6.2 Diritto di cancellazione e diritto di opposizione

6.2.1 Diritto di cancellazione (Diritto di essere dimenticati)

99. Se il responsabile del trattamento continua a trattare dati personali al di là del monitoraggio in tempo reale (ad esempio, la conservazione), l'interessato può chiedere la cancellazione dei dati personali ai sensi dell'articolo 17 GDPR.

100. Su richiesta, il responsabile del trattamento è tenuto a cancellare i dati personali senza indebito ritardo se si verifica una delle circostanze elencate all'articolo 17, paragrafo 1, RDPC (e nessuna delle eccezioni elencate all'articolo 17, paragrafo 3, RDPC). Ciò comprende l'obbligo di cancellare i dati personali quando non sono più necessari per lo scopo per il quale sono stati inizialmente memorizzati o quando il trattamento è illecito (si veda anche il *paragrafo 8 - Termini di conservazione e 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 ritirato (e non vi sono altre basi legali per il trattamento)
- per un *interesse legittimo*:
    - qualora l'interessato eserciti il diritto di opposizione (cfr. *punto 6.2.2*) e non sussistano motivi preminenti e legittimi per opporsi al trattamento, oppure
    - in caso di marketing diretto (inclusa la profilazione) ogni volta che l'interessato si oppone al trattamento.

101. Se il responsabile del trattamento ha reso pubblico il filmato video (ad es. trasmissione o streaming online), è necessario adottare misure ragionevoli per informare gli altri responsabili del trattamento (che ora trattano i dati personali in questione) della richiesta ai sensi dell'articolo 17, paragrafo 2, RDPC. Le misure ragionevoli dovrebbero comprendere misure tecniche, tenendo conto della tecnologia disponibile e dei costi di attuazione. Nella misura del possibile, il responsabile del trattamento deve notificare - all'atto della cancellazione dei dati personali - chiunque abbia ricevuto in precedenza i dati personali, ai sensi dell'articolo 19 GDPR.

102. Oltre all'obbligo del responsabile del trattamento di cancellare i dati personali su richiesta dell'interessato, il responsabile del trattamento è tenuto, in base ai principi generali del GDPR, a limitare i dati personali memorizzati (cfr. *sezione 8)*.

103. Per la videosorveglianza vale la pena di notare che, ad esempio, sfocando l'immagine senza la possibilità di recuperare retroattivamente i dati personali che l'immagine precedentemente contenuta, i dati personali sono considerati cancellati in conformità al GDPR.

> Esempio: Un negozio di alimentari ha problemi di vandalismo, in particolare all'esterno, e quindi utilizza la videosorveglianza all'esterno del suo ingresso in collegamento diretto con le pareti. Un passante chiede che i suoi dati personali siano cancellati da quel momento. Il controllore è tenuto a rispondere alla richiesta senza indebito ritardo e al più tardi entro un mese. Poiché i filmati in questione non rispondono più allo scopo per il quale erano stati inizialmente memorizzati (non si è verificato alcun atto vandalico nel periodo di tempo in cui l'interessato è passato), al momento della richiesta non vi è alcun interesse legittimo a memorizzare i dati che prevalga sugli interessi degli interessati. Il responsabile del trattamento deve cancellare i dati personali.

104.

6.2.2 Diritto di obiezione

105. Per la videosorveglianza basata su un *interesse legittimo* (articolo 6, paragrafo 1, lettera f), RDPP) o per la necessità di svolgere un compito di *interesse pubblico* (articolo 6, paragrafo 1, lettera e), RDPP), l'interessato ha il diritto - in qualsiasi momento - di opporsi, per motivi connessi alla sua situazione particolare, al trattamento ai sensi dell'articolo 21 RDPP. A meno che il responsabile del trattamento non dimostri motivi legittimi e convincenti che prevalgano sui diritti e sugli interessi dell'interessato, il trattamento dei dati dell'interessato che ha fatto obiezione deve allora cessare. Il responsabile del trattamento deve essere obbligato a rispondere alle richieste dell'interessato senza indebito ritardo e al più tardi entro un mese.

106. Nel contesto della videosorveglianza questa obiezione potrebbe essere fatta sia all'entrata, durante il tempo di permanenza, sia dopo l'uscita dall'area monitorata. In pratica ciò significa che, a meno che il responsabile del controllore non abbia validi motivi legittimi, il monitoraggio di un'area in cui potrebbero essere identificate persone fisiche è lecito solo se

(1) il controllore è in grado di interrompere immediatamente il trattamento dei dati personali quando richiesto, oppure

(2) l'area monitorata è limitata in modo così dettagliato che il responsabile del trattamento possa assicurare il consenso dell'interessato prima di entrare nell'area e non è un'area alla quale l'interessato, in quanto cittadino, ha diritto di accedere.

107. Queste linee guida non hanno lo scopo di identificare ciò che è considerato un interesse legittimo e *vincolante* (articolo 21 GDPR).

108. In caso di utilizzo della videosorveglianza a fini di marketing diretto, l'interessato ha il diritto di opporsi al trattamento in modo discrezionale, in quanto il diritto di opposizione è assoluto in tale contesto (articolo 21
(2) e (3) PILR).

Esempio: Un'azienda si trova in difficoltà a causa di violazioni della sicurezza all'ingresso del pubblico e utilizza la videosorveglianza per motivi di legittimo interesse, con lo scopo di catturare chi entra illegalmente. Un visitatore si oppone al trattamento dei suoi dati attraverso il sistema di videosorveglianza per motivi legati alla sua particolare situazione. La società tuttavia in questo caso respinge la richiesta con la spiegazione che i filmati memorizzati sono necessari a causa di un'indagine interna in corso, avendo quindi motivi validi e legittimi per continuare il trattamento dei dati personali.

109

7 OBBLIGHI DI TRASPARENZA E DI INFORMAZIONE[18]

110. È da tempo inerente alla legislazione europea sulla protezione dei dati che le persone interessate devono essere consapevoli del fatto che la videosorveglianza è in funzione. Essi dovrebbero essere informati in modo dettagliato sui luoghi monitorati[19]. Nell'ambito del GDPR gli obblighi generali di trasparenza e di informazione sono stabiliti dall'articolo 12 GDPR e seguenti. Le "Linee guida sulla trasparenza ai sensi del regolamento 2016/679 (WP260)" del gruppo di lavoro dell'articolo 29, approvate dall'EDPB il 25 maggio 2018, forniscono ulteriori dettagli. In linea con il par. 26, è l'articolo 13 GDPR, che si applica se i dati personali sono raccolti "[...] da una persona interessata tramite osservazione (ad esempio, utilizzando dispositivi automatici di acquisizione dei dati o software di acquisizione dei dati come le telecamere [...].

111. Alla luce del volume delle informazioni che devono essere fornite all'interessato, i responsabili del trattamento possono seguire un approccio a più livelli, scegliendo di utilizzare una combinazione di metodi per garantire la trasparenza (WP260, par. 35; WP89, par. 22). Per quanto riguarda la videosorveglianza, le informazioni più importanti dovrebbero essere visualizzate sul cartello stesso (primo livello), mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello).

7.1 Informazioni sul primo livello (segnale di avvertimento)

112. Il primo strato riguarda il modo primario in cui il responsabile del trattamento si relaziona per la prima volta con l'interessato. In questa fase, i controllori possono utilizzare un cartello di avvertimento con le relative informazioni. Le informazioni visualizzate possono essere fornite in combinazione con un'icona per dare, in modo facilmente visibile, comprensibile e chiaramente leggibile, una visione d'insieme significativa del trattamento previsto (articolo 12
(7) PILR). Il formato delle informazioni deve essere adattato alla posizione individuale (WP89 par. 22).

7.1.1 Posizionamento del segnale di avvertimento

113. Le informazioni devono essere posizionate in modo tale che l'interessato possa riconoscere facilmente le circostanze della sorveglianza prima di entrare nell'area monitorata (approssimativamente all'altezza degli occhi). Non è necessario rivelare la posizione della telecamera, purché non vi siano dubbi su quali aree siano soggette a monitoraggio e il contesto della sorveglianza sia chiarito in modo inequivocabile (WP 89, par. 22). L'interessato deve essere in grado di stimare quale area viene catturata da una telecamera in modo da poter evitare la sorveglianza o adattare il proprio comportamento, se necessario.

7.1.2 Contenuto del primo strato

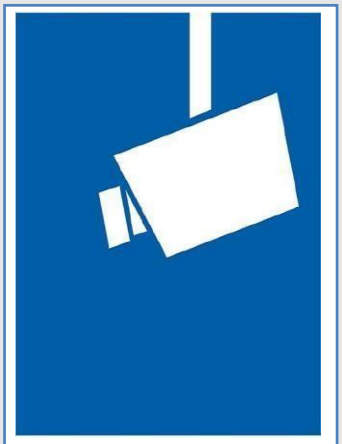
114. Le informazioni del primo livello (segnale di avvertimento) dovrebbero in genere trasmettere le informazioni più importanti, ad esempio i dettagli delle finalità del trattamento, l'identità del responsabile del trattamento e l'esistenza dei diritti dell'interessato, insieme alle informazioni sui maggiori impatti del trattamento[20]. Ciò può includere, ad esempio, gli interessi legittimi perseguiti dal responsabile del trattamento (o da un terzo) e i dati di contatto del responsabile della protezione dei dati (se del caso). Deve anche fare riferimento al secondo livello di informazioni più dettagliato e dove e come trovarle.

115. Inoltre il cartello dovrebbe contenere anche tutte le informazioni che potrebbero sorprendere l'interessato (WP260, par. 38). Potrebbe trattarsi, ad esempio, di trasmissioni a terzi, in particolare se si trovano

[18] Potrebbero applicarsi requisiti specifici nella legislazione nazionale.
[19] Cfr. WP859, Parere 4/2004 sul trattamento dei dati personali mediante videosorveglianza del gruppo di lavoro "Articolo 29").
[20] Vedi WP260, par. 38.

al di fuori dell'UE, e il periodo di conservazione. Se questa informazione non viene indicata, l'interessato deve potersi fidare del fatto che ci sia solo un monitoraggio in tempo reale (senza registrazione o trasmissione di dati a terzi).

Esempio (suggerimento non vincolante):



Videosorveglianza!

Identità del controllore e, se del caso, del suo rappresentante: Dati di contatto, compreso il responsabile della protezione dei dati (se del caso):

Informazioni sul trattamento che ha il maggiore impatto sull'interessato (ad es. periodo di conservazione o monitoraggio in diretta, pubblicazione o trasmissione a terzi di filmati video):

Scopo(i) della videosorveglianza:

Ulteriori informazioni sono disponibili:
- tramite avviso
- presso la nostra reception/ informazioni clienti/ registrazione
- via internet (URL)...

Diritti degli interessati: In qualità di interessato avete diversi diritti da esercitare, in particolare il diritto di chiedere al responsabile del trattamento l'accesso o la cancellazione dei vostri dati personali.

Per i dettagli su questa videosorveglianza, compresi i vostri diritti, consultate le informazioni complete fornite dal controllore attraverso le opzioni presentate a sinistra.

116.

7.2 Informazioni sul secondo livello

117. Anche le informazioni del secondo livello devono essere messe a disposizione in un luogo facilmente accessibile all'interessato, ad esempio come scheda informativa completa disponibile in una postazione centrale (ad es. sportello informazioni, reception o cassa) o esposta su un poster facilmente accessibile. Come già detto, il segnale di avvertimento del primo strato deve fare riferimento in modo chiaro alle informazioni del secondo strato. Inoltre, è meglio se le informazioni del primo livello si riferiscono a una fonte digitale (ad esempio il codice QR o l'indirizzo del sito web) del secondo livello. Tuttavia, le informazioni dovrebbero essere facilmente disponibili anche in forma non digitale. Dovrebbe essere possibile accedere alle informazioni del secondo livello senza entrare nell'area censita, soprattutto se le informazioni sono fornite in formato digitale (ciò può essere realizzato ad esempio tramite un link). Un altro mezzo appropriato potrebbe essere un numero di telefono che può essere chiamato. In ogni caso, le informazioni fornite devono contenere tutto ciò che è obbligatorio ai sensi dell'articolo 13 GDPR.

118. Oltre a queste opzioni, e anche per renderle più efficaci, l'EDPB promuove l'uso di mezzi tecnologici per fornire informazioni alle persone interessate. Ciò può includere, ad esempio, la geo-localizzazione delle telecamere e l'inserimento di informazioni nelle applicazioni di mappatura o nei siti web, in modo che gli individui possano facilmente, da un lato, identificare e specificare le fonti video relative all'esercizio dei loro diritti e, dall'altro, ottenere informazioni più dettagliate sull'operazione di elaborazione.

> Esempio: Il proprietario di un negozio sta monitorando il suo negozio. Per rispettare l'articolo 13 è sufficiente posizionare un cartello di avvertimento in un punto facilmente visibile all'ingresso del suo negozio, che contiene le informazioni del primo livello. Inoltre, deve fornire un foglio informativo contenente le informazioni del secondo livello alla cassa o in qualsiasi altro luogo centrale e facilmente accessibile nel suo negozio.

119.

8 PERIODI DI CONSERVAZIONE E OBBLIGO DI CANCELLAZIONE

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

121. Se i dati personali sono necessari per la memorizzazione o meno, devono essere controllati entro un periodo di tempo limitato. In generale, gli scopi legittimi della videosorveglianza sono spesso la protezione della proprietà o la conservazione delle prove. Di solito i danni che si sono verificati possono essere riconosciuti entro uno o due giorni. Per facilitare la dimostrazione del rispetto del quadro normativo sulla protezione dei dati è nell'interesse del responsabile del trattamento prendere in anticipo disposizioni organizzative (ad es. nominare, se necessario, un rappresentante per la proiezione e la messa in sicurezza del materiale video). Tenendo conto dei principi dell'articolo 5, paragrafo 1, lettera c) e
e) GDPR, ossia la minimizzazione dei dati e la limitazione della loro conservazione, i dati personali dovrebbero nella maggior parte dei casi (ad esempio per rilevare atti vandalici) essere cancellati, idealmente in modo automatico, dopo pochi giorni. Quanto più lungo è il periodo di conservazione stabilito (soprattutto se superiore a 72 ore), tanto più si deve argomentare la legittimità dello scopo e la necessità di conservazione. Se il responsabile del trattamento utilizza la videosorveglianza non solo per monitorare i propri locali, ma intende anche memorizzare i dati, il responsabile del trattamento deve assicurarsi che la memorizzazione sia effettivamente necessaria per raggiungere lo scopo. In caso affermativo, il periodo di conservazione deve essere chiaramente definito e impostato individualmente per ogni scopo particolare. È responsabilità del controllore definire il periodo di conservazione secondo i principi di necessità e proporzionalità e dimostrare il rispetto delle disposizioni del GDPR.

> Esempio: Il proprietario di un piccolo negozio di solito si accorge di eventuali atti di vandalismo il giorno stesso. Di conseguenza, è sufficiente un periodo di conservazione regolare di 24 ore. I fine settimana chiusi o i giorni festivi più lunghi possono tuttavia essere motivi per un periodo di conservazione più lungo. Se venisse rilevato un danno, potrebbe anche essere necessario conservare le riprese video per un periodo più lungo al fine di intraprendere un'azione legale contro il trasgressore.

122.

9 MISURE TECNICHE E ORGANIZZATIVE

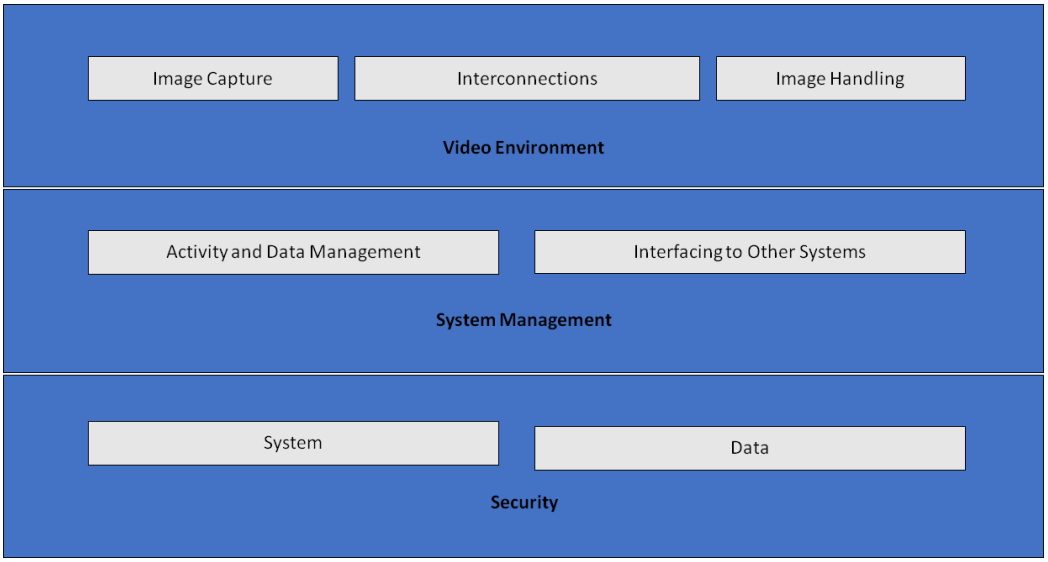
123. Come stabilito dall'articolo 32, paragrafo 1, RDPP, il trattamento dei dati personali durante la videosorveglianza non solo deve essere legalmente consentito, ma i responsabili del trattamento e gli incaricati del trattamento devono anche proteggerli adeguatamente. **Le misure organizzative e tecniche** attuate devono essere **proporzionate ai rischi per i diritti e le libertà delle persone fisiche**, derivanti da distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso ai dati di videosorveglianza. Ai sensi degli articoli 24 e 25 del GDPR, i responsabili del trattamento devono attuare misure tecniche e organizzative anche al fine di salvaguardare tutti i principi di protezione dei dati durante il trattamento e stabilire i mezzi per l'esercizio dei diritti degli interessati, come definiti negli articoli 15-22 del GDPR. I responsabili del trattamento dei dati dovrebbero adottare un quadro interno e politiche che garantiscano tale attuazione sia al momento della determinazione dei mezzi per il trattamento sia al momento del trattamento stesso, compresa l'esecuzione di valutazioni d'impatto sulla protezione dei dati quando necessario

9.1 Panoramica del sistema di videosorveglianza

124. Un sistema di videosorveglianza (VSS)[21] è costituito da dispositivi analogici e digitali e da un software per catturare le immagini di una scena, gestire le immagini e visualizzarle ad un operatore. I suoi componenti sono raggruppati nelle seguenti categorie:

- Ambiente video: cattura delle 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 tutte le trasmissioni di dati all'interno dell'ambiente video, cioè le connessioni e le comunicazioni. Esempi di connessioni sono i cavi, le reti digitali e le trasmissioni senza fili. Le comunicazioni descrivono tutti i segnali di dati video e di controllo, che possono essere digitali o analogici,
    - La gestione delle immagini comprende l'analisi, la memorizzazione e la 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 comprende la gestione dei comandi degli operatori e delle attività generate dal sistema (procedure di allarme, avvisi agli operatori),
    - Le interfacce con altri sistemi possono includere il collegamento ad altri sistemi di sicurezza (controllo accessi, allarme antincendio) e non di sicurezza (sistemi di gestione degli edifici, riconoscimento automatico delle targhe).
- La sicurezza VSS consiste nella riservatezza, integrità e disponibilità del sistema e dei dati:
    - La sicurezza del sistema comprende la sicurezza fisica di tutti i componenti del sistema e il controllo dell'accesso al VSS,
    - La sicurezza dei dati comprende la prevenzione della perdita o della manipolazione dei dati.

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



125.

Figura 1- sistema di videosorveglianza

9.2 Protezione dei dati in base alla progettazione e per default

126. Come stabilito dall'articolo 25 GDPR, i responsabili del trattamento devono attuare misure tecniche e organizzative adeguate per la protezione dei dati non appena pianificano la videosorveglianza - prima di iniziare la raccolta e l'elaborazione delle riprese video. Questi principi sottolineano la necessità di tecnologie integrate per migliorare la privacy, di impostazioni predefinite che riducano al minimo il trattamento dei dati e di fornire gli strumenti necessari che consentano la massima protezione possibile dei dati personali[22].

127. I responsabili del trattamento dovrebbero integrare la protezione dei dati e la tutela della vita privata non solo nelle specifiche di progettazione della tecnologia, ma anche nelle pratiche organizzative. Quando si tratta di pratiche organizzative, il controllore 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 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 difetto ai sensi dell'articolo 25, paragrafo 2, GDPR, integrità e riservatezza, responsabilità, ecc. Nel caso in cui un controllore intenda acquistare un sistema di videosorveglianza commerciale, il controllore deve includere questi requisiti nelle specifiche di acquisto. Il controllore deve garantire il rispetto di questi requisiti applicandoli a tutti i componenti del sistema e a tutti i dati da esso trattati, durante il loro intero ciclo di vita.

9.3 Esempi concreti di misure rilevanti

128. La maggior parte delle misure che possono essere utilizzate per la videosorveglianza, soprattutto quando si utilizzano apparecchiature e software digitali, non differiscono da quelle utilizzate in altri sistemi informatici. Tuttavia, indipendentemente dalla soluzione scelta, il controllore deve proteggere adeguatamente tutti i componenti di un sistema di videosorveglianza e i dati in tutte le fasi, cioè durante la conservazione (dati a riposo), la trasmissione (dati in transito) e elaborazione (dati in uso). Per questo è necessario che i controllori e i processori combinino misure organizzative e tecniche.

129. Nella scelta delle soluzioni tecniche, il controllore dovrebbe considerare tecnologie rispettose della privacy anche perché migliorano la sicurezza. Esempi di tali tecnologie sono i sistemi che consentono

[22] WP 168, Parere sul "Futuro della privacy", contributo congiunto del Gruppo di lavoro "Articolo 29 - Protezione dei dati personali" e del Gruppo di lavoro "Polizia e giustizia" alla consultazione della Commissione europea sul quadro giuridico per il diritto fondamentale alla protezione dei dati personali (adottato il 1°dicembre 2009).

di mascherare o rimescolare aree che non sono rilevanti per la sorveglianza, o il montaggio di immagini di terze persone, quando si forniscono riprese video ai soggetti interessati[23]. D'altra parte, le soluzioni selezionate non dovrebbero fornire funzioni che non siano necessarie (ad esempio, movimento illimitato delle telecamere, capacità di zoom, trasmissione radio, analisi e registrazioni audio). Le funzioni fornite, ma non necessarie, devono essere disattivate.

130. Su questo argomento è disponibile molta letteratura, comprese le norme internazionali e le specifiche tecniche sulla sicurezza fisica dei sistemi multimediali[24] e la sicurezza dei sistemi informatici in generale[25]. Pertanto, questa sezione fornisce solo una panoramica di alto livello su questo argomento.

9.3.1 Misure organizzative

131. A parte una potenziale DPIA necessaria (cfr. *Sezione 10*), i controllori 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.
- Scopo e portata del progetto di videosorveglianza.
- 25. Uso appropriato e vietato (dove e quando la videosorveglianza è consentita e dove e quando non lo è; ad es. uso di telecamere nascoste e audio in aggiunta alla registrazione video)[26].
- Misure di trasparenza di cui alla *Sezione 7 (Trasparenza e obblighi di informazione).*
- Come viene registrato il video e per quale durata, compresa l'archiviazione delle registrazioni video relative agli incidenti di sicurezza.
- Chi deve seguire una formazione pertinente e quando.
- Chi ha accesso alle registrazioni video e per quali scopi.
- Procedure operative (ad es. da chi e da dove viene monitorata la videosorveglianza, cosa fare in caso di violazione dei dati).
- Quali sono le procedure che i soggetti esterni devono seguire per richiedere le registrazioni video e le procedure per negare o concedere tali richieste.
- Procedure per l'approvvigionamento, l'installazione e la manutenzione dei VSS.
- Gestione degli incidenti e procedure di recupero.

9.3.2 Misure tecniche

132. **Per sicurezza del sistema** si intende la **sicurezza fisica** di tutti i componenti del sistema e l'integrità del sistema, cioè la **protezione e la resilienza sotto l'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 chi ne ha diritto), **integrità** (prevenzione della perdita o della manipolazione dei dati) e **disponibilità** (i dati sono accessibili quando sono necessari).

133. **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, catastrofi naturali, catastrofi antropiche e danni accidentali (ad esempio, da sovratensioni elettriche, temperature estreme e caffè versato). Nel caso di sistemi analogici, la sicurezza fisica gioca il ruolo principale nella loro protezione.

134. **La sicurezza del sistema e dei dati, cioè** la protezione contro interferenze intenzionali e non intenzionali con il suo normale funzionamento, può includere:

- Protezione dell'intera infrastruttura VSS (comprese le telecamere remote, il cablaggio e l'alimentazione) contro manomissioni fisiche e furti.
- Protezione della trasmissione di filmati con canali di comunicazione sicuri contro le

[23] L'uso di tali tecnologie può anche essere obbligatorio in alcuni casi 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 dentro e fuori uso.
[25] ISO/IEC 27000 - Serie di sistemi di gestione della sicurezza delle informazioni.
[26] Ciò può dipendere dalle leggi nazionali e dalle normative di settore.

intercettazioni

- 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.

135. **Il controllo degli accessi** assicura che solo le persone autorizzate possano accedere al sistema e ai dati, mentre ad altri è impedito l'accesso. Le misure che supportano il controllo dell'accesso fisico e logico includono:

- Garantire che tutti i locali in cui viene effettuato il monitoraggio tramite videosorveglianza e in cui sono conservati i filmati siano protetti contro l'accesso non sorvegliato da parte di terzi.
- Posizionare i monitor in modo tale (soprattutto quando si trovano in aree aperte, come una reception) in modo che solo gli operatori autorizzati possano vederli.
- Le procedure per la concessione, la modifica e la revoca dell'accesso fisico e logico sono definite e applicate.
- Vengono implementati metodi e mezzi di autenticazione e autorizzazione dell'utente, tra cui ad esempio la lunghezza delle password e la frequenza di modifica.
- Le azioni eseguite dall'utente (sia al sistema che ai dati) vengono registrate e riviste regolarmente.
- Il monitoraggio e l'individuazione dei guasti di accesso viene effettuato in modo continuo e i punti deboli identificati vengono affrontati il più presto possibile.

10 VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

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

137. Le linee guida sulla valutazione d'impatto della protezione dei dati[27] forniscono ulteriori consigli ed esempi più dettagliati relativi alla videosorveglianza (ad esempio riguardo all'"uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade"). L'articolo 35 (4) GDPR prevede che ogni autorità di controllo pubblichi un elenco dei tipi di trattamenti soggetti a DPIA obbligatoria all'interno del proprio paese. Questi elenchi si trovano di solito sui siti web delle autorità. Dati gli scopi tipici della videosorveglianza (protezione delle persone e dei beni, individuazione, prevenzione e controllo dei reati, raccolta di prove e identificazione biometrica dei sospetti), è ragionevole supporre che molti casi di videosorveglianza richiedano una DPIA. Pertanto, i responsabili del trattamento dei dati dovrebbero consultare attentamente questi documenti per determinare se tale valutazione è necessaria e, se necessario, effettuarla. L'esito della DPIA eseguita dovrebbe determinare la scelta da parte del responsabile del trattamento delle misure di protezione dei dati attuate.

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

Per il Comitato europeo per la protezione dei dati Il presidente

(Andrea Jelinek)

[27] WP248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) e determinare se l'elaborazione è "suscettibile di comportare un rischio elevato" ai fini del regolamento 2016/679. - approvato dall'EDPB