Riunione plenaria dell'EDPB, 09-10 luglio 2019

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

Versione per consultazione pubblica

Adottato il 10 luglio 2019

Sommario

Pagina 4

Il comitato europeo per la protezione dei dati

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

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

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

HA ADOTTATO LE SEGUENTI LINEE GUIDA

1. INTRODUZIONE

1. L'uso intensivo di dispositivi video ha un impatto sul comportamento dei cittadini. Implementazione significativa di tali strumenti in molte sfere della vita degli individui eserciteranno un'ulteriore pressione sull'individuo impedire il rilevamento di ciò che potrebbe essere percepito come anomalia. Di fatto, queste tecnologie possono limitare le possibilità di movimento anonimo e uso anonimo dei servizi e generalmente limitano il possibilità di rimanere inosservati. Le implicazioni sulla protezione dei dati sono enormi.

2. Mentre le persone potrebbero sentirsi a proprio agio con la videosorveglianza impostata per un determinato scopo di sicurezza ad esempio, devono essere prese garanzie per evitare qualsiasi uso improprio di dati totalmente diversi e - ai dati soggetto - scopi imprevisti (ad es. scopo di marketing, monitoraggio delle prestazioni dei dipendenti, ecc.). Nel Inoltre, molti strumenti sono ora implementati per sfruttare le immagini catturate e trasformarle in tradizionali telecamere in telecamere intelligenti. La quantità di dati generati dal video, combinati con questi strumenti e le tecniche aumentano i rischi di uso secondario (se correlati o meno allo scopo originariamente assegnato al sistema) o anche i rischi di uso improprio. I principi generali del GDPR (articolo 5), dovrebbero essere sempre attentamente considerati quando si tratta di videosorveglianza.

3. I sistemi di videosorveglianza in molti modi cambiano il modo in cui i professionisti del settore privato e pubblico il settore interagisce in luoghi privati o pubblici allo scopo di migliorare la sicurezza, ottenere pubblico analisi, fornitura di pubblicità personalizzata, ecc. La videosorveglianza è diventata altamente performante attraverso la crescente implementazione di analisi video intelligenti. Queste tecniche possono essere di più

invadente (ad es. tecnologie biometriche complesse) o meno invadente (ad es. algoritmi di conteggio semplici).
Restare anonimi e preservare la propria privacy è in generale sempre più difficile. I dati
i problemi di protezione sollevati in ogni situazione possono differire, così come l'analisi legale quando si utilizza uno o il
altra di queste tecnologie.

4. Oltre ai problemi di privacy, ci sono anche rischi legati a possibili malfunzionamenti di questi dispositivi e
i pregiudizi che possono indurre. I ricercatori riferiscono che il software utilizzato per l'identificazione facciale, il riconoscimento,
o l'analisi viene eseguita in modo diverso in base all'età, al sesso e all'etnia della persona che sta identificando.
Gli algoritmi si comporterebbero in base a dati demografici diversi, pertanto la propensione al riconoscimento facciale minaccia
rafforzare i pregiudizi della società. Questo è il motivo per cui i responsabili del trattamento dei dati devono anche garantire tale biometria

Pagina 5

il trattamento dei dati derivante dalla videosorveglianza è soggetto a regolare valutazione della sua rilevanza e
sufficienza delle garanzie fornite.

5. La videosorveglianza non è di default una necessità quando esistono altri mezzi per raggiungere il sottostante
scopo. Altrimenti rischiamo un cambiamento nelle norme culturali che porta all'accettazione della mancanza di privacy come
l'inizio generale.

6. Queste linee guida mirano a fornire indicazioni su come applicare il GDPR in relazione al trattamento personale
dati attraverso dispositivi video. Gli esempi non sono esaustivi, è possibile applicare il ragionamento generale
tutte le potenziali aree di utilizzo.

2 CAMPO DI APPLICAZIONE [1]

2.1 Dati personali

7. Monitoraggio automatico sistematico di uno spazio specifico con mezzi ottici o audiovisivi, principalmente per
scopi di protezione della proprietà, o per proteggere la vita e la salute dell'individuo, sono diventati significativi
fenomeno dei nostri giorni. Questa attività comporta la raccolta e la conservazione di immagini o audiovisivi
informazioni su tutte le persone che entrano nello spazio monitorato identificabili sulla base del loro aspetto o
altri elementi specifici. L'identità di queste persone può essere stabilita sulla base di questi dettagli. esso
consente inoltre l'ulteriore trattamento dei dati personali per quanto riguarda la presenza e il comportamento delle persone nel dato
spazio. Il potenziale rischio di uso improprio di questi dati aumenta in relazione alla dimensione del monitorato
spazio, nonché al numero di persone che frequentano lo spazio. Questo fatto è riflesso dal Generale
Regolamento sulla protezione dei dati di cui all'articolo 35, paragrafo 3, lettera c), che prevede lo svolgimento di una protezione dei dati
valutazione di impatto in caso di monitoraggio sistematico di un'area accessibile al pubblico su larga scala, come
nonché all'articolo 37, paragrafo 1, lettera b), che impone ai responsabili del trattamento di designare un responsabile della protezione dei dati, se il
il trattamento per sua natura comporta un monitoraggio regolare e sistematico degli interessati.

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

> Esempio: il GDPR non è applicabile per le fotocamere false (ovvero qualsiasi fotocamera che non funziona
> come fotocamera e quindi non elabora alcun dato personale). *Tuttavia, in alcuni Stati membri*
> *potrebbe essere soggetto ad altra legislazione.*
>
> Esempio: le registrazioni da un'altitudine elevata rientrano nell'ambito di applicazione del GDPR solo se in
> circostanze in cui i dati trattati possono essere correlati a una persona specifica.
>
> Esempio: una videocamera è integrata in un'auto per fornire assistenza al parcheggio. Se la fotocamera lo è
> costruito o adattato in modo tale da non raccogliere alcuna informazione relativa a
> persona fisica (come 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 di dati personali da parte delle autorità competenti a fini di prevenzione,
indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali,

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

compresa la protezione e la prevenzione delle minacce alla pubblica sicurezza, rientra nel campo di applicazione 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 nel corso di a attività puramente personali o domestiche, che possono includere anche attività online, non rientrano nell'ambito di applicazione di GDPR. [2]

12. Questa disposizione - la cosiddetta esenzione delle famiglie - nel contesto della videosorveglianza deve essere interpretato in modo restrittivo. Quindi, come considerato dalla Corte di giustizia europea, la cosiddetta "famiglia" esenzione "deve *essere " interpretata come relativa esclusivamente alle attività svolte nel corso del vita privata o familiare delle persone, il che chiaramente non è il caso del trattamento dei dati personali consistente nella pubblicazione su Internet in modo tale che tali dati siano resi accessibili a un numero indefinito di persone* ". [3] Inoltre, se si tratta di un sistema di videosorveglianza, nella misura in cui comporta la costante registrazione e archiviazione di dati personali e copertine, " *anche parzialmente, uno spazio pubblico ed è di conseguenza diretto verso l'esterno dall'impostazione privata della persona che elabora i dati in quel modo, non può essere considerata un'attività puramente "personale o domestica" ai fini del articolo 3, paragrafo 2, secondo trattino, della direttiva 95/46 "* [4] .

13. Per quanto riguarda i dispositivi video gestiti all'interno dei locali di un privato, potrebbe rientrare nel campo di applicazione esenzione familiare. Dipenderà da diversi fattori, che tutti devono essere considerati per raggiungere una conclusione. Oltre agli elementi sopra menzionati identificati dalle sentenze della CGE, l'utente del video la sorveglianza a casa deve verificare se ha qualche tipo di relazione personale con i dati soggetto, se la scala o la frequenza della sorveglianza suggerisce un tipo di attività professionale dalla sua parte e del potenziale impatto negativo della sorveglianza sugli interessati. La presenza di uno qualsiasi dei suddetti elementi non suggerisce necessariamente che l'elaborazione sia al di fuori del campo di applicazione dell'esenzione per le famiglie, è necessaria una valutazione globale per questo determinazione.

2 Vedi anche considerando 18.

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

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

Esempio: un turista sta registrando video sia tramite il suo telefono cellulare che tramite un videocamera per documentare le sue vacanze. Mostra le riprese ad amici e parenti ma non lo fa renderlo accessibile a un numero indefinito di persone. Questo sarebbe caduto sotto la famiglia esenzione.

Esempio: un mountainbike in discesa vuole registrare la sua discesa con una actioncam. Lei è cavalcare in una zona remota e prevede solo di utilizzare le registrazioni per il suo intrattenimento personale a casa. Ciò rientrerebbe nell'esenzione delle famiglie.

Esempio: qualcuno sta monitorando e registrando il proprio giardino. La proprietà è recintata e solo il controllore stesso e la sua famiglia entrano regolarmente nel giardino. Questo rientrerebbe nell'esenzione delle famiglie, a condizione che la videosorveglianza no estendersi anche parzialmente a uno spazio pubblico o proprietà vicina.

14.

3 LEGGE DEL TRATTAMENTO

15. Prima dell'uso, le finalità del trattamento devono essere specificate in dettaglio (articolo 5, paragrafo 1, lettera b)). video la sorveglianza può servire a molti scopi, ad esempio la protezione di proprietà e altri beni, la raccolta di prove per azioni civili. [5] Questi scopi di monitoraggio dovrebbero essere documentati per iscritto (articolo 5, paragrafo 2) e necessari da specificare per ogni telecamera di sorveglianza in uso. Telecamere utilizzate per lo stesso scopo da a un singolo controller può essere documentato insieme, purché ogni telecamera in uso ne abbia una documentata scopo. Inoltre, gli interessati devono essere informati delle finalità del trattamento in questione conformemente all'articolo 13 (*cfr. sezione 7, Trasparenza e obblighi di informazione*). video la sorveglianza basata sul mero scopo di "sicurezza" o "per la tua sicurezza" non è sufficientemente specifica (Articolo 5, paragrafo 1, lettera b)). È inoltre contrario al principio che i dati personali devono essere trattati in modo lecito, equo e trasparente nei confronti dell'interessato (cfr. l'articolo 5, paragrafo 1, lettera a)).

16. In linea di principio, ogni base giuridica ai sensi dell'articolo 6, paragrafo 1, può fornire una base giuridica per l'elaborazione dei video dati di sorveglianza. Ad esempio, si applica l'articolo 6, paragrafo 1, lettera c), laddove la legislazione nazionale preveda l'obbligo di video sorveglianza. [6] Tuttavia, nella pratica, le disposizioni che hanno più probabilità di essere utilizzate sono

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

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

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

3.1 Legittimo interesse, articolo 6, paragrafo 1, lettera f)

17. La valutazione giuridica dell'articolo 6, paragrafo 1, lettera f), dovrebbe essere basata sui seguenti criteri in conformità con Considerando 47.

5 Le regole sulla raccolta delle prove per le rivendicazioni civili variano negli Stati membri.

6 Queste linee guida non analizzano o entrano nei dettagli della legislazione nazionale che potrebbero differire tra loro stati membri.

3.1.1 Esistenza di interessi legittimi

18. La videosorveglianza è lecita se è necessaria al fine di soddisfare lo scopo di un interesse legittimo perseguito da un responsabile del trattamento o da terzi, a meno che tali interessi non siano ignorati dall'interessato interessi o diritti e libertà fondamentali (articolo 6, paragrafo 1, lettera f)). Legittimi interessi perseguiti da a il responsabile del trattamento o una terza parte può essere legale, [7] interessi economici o non rilevanti. [8] Tuttavia, il controller dovrebbe considerare che se l'interessato si oppone alla sorveglianza ai sensi dell'articolo 21, il il responsabile del trattamento può procedere con la videosorveglianza dell'interessato solo se *convincente* interesse legittimo che prevalga sugli interessi, i diritti e le libertà dell'interessato o per istituzione, esercizio o difesa di rivendicazioni legali.

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

20. L'interesse legittimo deve essere di esistenza reale e deve essere un problema attuale (cioè non deve esserlo immaginario o speculativo) [9] . Una situazione di sofferenza nella vita reale deve essere a portata di mano - come danni o gravi incidenti in passato - prima di iniziare la sorveglianza. Alla luce del principio di responsabilità, si consiglia ai responsabili del trattamento di documentare gli incidenti rilevanti (data, modalità, perdita finanziaria) e accuse penali correlate. Questi incidenti documentati possono essere una prova evidente dell'esistenza di a interesse legittimo.

    Esempio: il proprietario di un negozio desidera aprire un nuovo negozio e desidera installare una videosorveglianza sistema. Può mostrare, presentando statistiche, che c'è un'alta aspettativa di atti vandalici il vicino quartiere. Inoltre, è utile l'esperienza dei negozi vicini. Non è necessario che si sia verificato un danno al controllore in questione. Tuttavia non lo è sufficiente per presentare statistiche nazionali o generali sul crimine senza analizzare l'area in questione o i pericoli per questo negozio specifico.

21.

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

23. .Il GDPR afferma inoltre chiaramente che le autorità pubbliche non possono basare il loro trattamento sulla base di interesse legittimo, purché svolgano i loro compiti, articolo 6, paragrafo 1, frase 2.

3.1.2 Necessità del trattamento

24. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per i quali sono trattati ("minimizzazione dei dati"), cfr. l'articolo 5, paragrafo 1, lettera c). Prima di installare un video sistema di sorveglianza che il responsabile del trattamento dovrebbe sempre esaminare criticamente se questa misura è inizialmente adatta a raggiungere l'obiettivo desiderato, e in secondo luogo adeguato e necessario per i suoi scopi. Video sorveglianza le misure dovrebbero essere scelte solo se lo scopo del trattamento non può ragionevolmente essere raggiunto da altri mezzi meno invasivi per i diritti e le libertà fondamentali dell'interessato.

25. Data la situazione in cui un controller vuole prevenire reati connessi alla proprietà, invece di installare a sistema di videosorveglianza il controller potrebbe anche adottare misure di sicurezza alternative come la scherma la proprietà, installando pattuglie regolari del personale di sicurezza, usando i guardiani, fornendo meglio

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

8 vedi wp 217, gruppo di lavoro articolo 29.

9 vedi wp 217, gruppo di lavoro articolo 29, pag. 24 seq.

illuminazione, installazione di serrature di sicurezza, finestre e porte a prova di manomissione o applicazione di rivestimento antigraffiti o lamine alle pareti. Tali misure possono essere efficaci quanto i sistemi di videosorveglianza contro furto con scasso, furto e atti vandalici.

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

27. In generale, la necessità di utilizzare la videosorveglianza per proteggere i locali dei controllori termina al confini della proprietà .10 Tuttavia, ci sono casi in cui la sorveglianza della proprietà non è sufficiente per una protezione efficace. In alcuni casi individuali potrebbe essere necessario superare il video sorveglianza nelle immediate vicinanze dei locali. In questo contesto, il controller dovrebbe considerare mezzi fisici e tecnici, ad esempio bloccare o pixelare aree non rilevanti.

> Esempio: una libreria vuole proteggere le sue premesse dal vandalismo. In generale, telecamere dovrebbe girare solo i locali perché non è necessario guardare i vicini locali o aree pubbliche circostanti i locali della libreria a tale scopo.

28.

29. Sorgono anche domande sulla necessità del trattamento riguardo al modo in cui le prove sono conservate. Nel in alcuni casi potrebbe essere necessario utilizzare soluzioni black box in cui il filmato viene automaticamente eliminato dopo un certo periodo di conservazione e vi si accede solo in caso di incidente. In altre situazioni potrebbe non esserlo essere necessario per registrare il materiale video, ma più appropriato per utilizzare il monitoraggio in tempo reale anziché. Anche la decisione tra soluzioni black box e monitoraggio in tempo reale dovrebbe essere basata lo 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 di più invadente rispetto alla memorizzazione e alla cancellazione automatica del materiale dopo un periodo di tempo limitato. I dati il principio di minimizzazione deve essere considerato in questo contesto (articolo 5, paragrafo 1, lettera c)). Dovrebbe anche essere tenuto a mente che potrebbe essere possibile che il responsabile del trattamento possa utilizzare il personale di sicurezza anziché la videosorveglianza che sono in grado di reagire e intervenire immediatamente.

3.1.3 Bilanciamento degli interessi

30. Presumendo che la videosorveglianza sia necessaria per proteggere gli interessi legittimi di un responsabile del trattamento, a il sistema di videosorveglianza può essere messo in funzione solo se gli interessi legittimi del responsabile del trattamento o quelli di terzi (es. protezione della proprietà o integrità fisica) non sono sostituiti da interessi o diritti e libertà fondamentali dell'interessato. Il controller deve considerare 1) in che misura il monitoraggio incide sugli interessi legittimi, sui diritti fondamentali e sulle libertà di persone fisiche e 2) se ciò causa violazioni o conseguenze negative in relazione all'interessato diritti. In effetti, il bilanciamento degli interessi è obbligatorio. Diritti e libertà fondamentali da un lato e gli interessi legittimi del responsabile del trattamento devono invece essere valutati ed equilibrati attentamente.

10 Ciò potrebbe anche essere soggetto alla legislazione nazionale in alcuni Stati membri.

Pagina 10

Esempio: una società di parcheggio privata ha documentato problemi ricorrenti con furti nel macchine parcheggiate. L'area di parcheggio è uno spazio aperto e può essere facilmente accessibile da chiunque, ma lo è chiaramente contrassegnati con cartelli e blocchi stradali che circondano lo spazio. La compagnia di parcheggio avere un interesse legittimo (prevenire i furti nelle auto del cliente) per monitorare l'area durante l'ora del giorno in cui si verificano problemi. Gli interessati sono monitorati in a periodo di tempo limitato, non si trovano nell'area per scopi ricreativi ed è anche loro interesse a prevenire furti. È nell'interesse delle persone interessate da non monitorare questo caso è annullato dall'interesse legittimo del responsabile del trattamento.

Esempio: un ristorante decide di installare videocamere nei bagni per controllare l'ordine delle strutture sanitarie. In questo caso i diritti degli interessati prevalgono chiaramente sul interesse del controller, quindi le telecamere non possono essere installate lì.

31.

3.1.3.1 Prendere decisioni caso per caso

32. Poiché il bilanciamento degli interessi è obbligatorio ai sensi del regolamento, la decisione deve essere presa caso per caso (cfr. l'articolo 6, paragrafo 1, lettera f)). Fare riferimento a situazioni astratte o confrontare casi simili a l'un l'altro è insufficiente. Il responsabile del trattamento deve valutare i rischi di intrusione della persona interessata diritti; qui il criterio decisivo è l'intensità di intervento per i diritti e le libertà della individuale.

33. L'intensità può essere definita tra l'altro dal tipo di informazioni raccolte (contenuto delle informazioni), la portata (densità delle informazioni, estensione spaziale e geografica), il numero di interessati interessata, sia come numero specifico sia come percentuale della popolazione interessata, la situazione in questione domanda, gli interessi reali del gruppo di interessati, mezzi alternativi, nonché dalla natura e portata della valutazione dei dati.

34. Importanti fattori di bilanciamento possono essere la dimensione dell'area, che è sotto sorveglianza e la quantità di soggetti interessati sotto sorveglianza. L'uso della videosorveglianza in un'area remota (ad es. Per osservare la fauna selvatica o per proteggere le infrastrutture critiche come un'antenna radio di proprietà privata) deve essere valutata diversamente dalla videosorveglianza in una zona pedonale o in un centro commerciale.

1. Esempio: se è installata una dash cam (ad esempio allo scopo di raccogliere prove in caso di un incidente), è importante assicurarsi che anche questa videocamera non stia registrando costantemente il traffico come persone che si trovano vicino a 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 dati diritti del soggetto. [11]

[11]

3.1.3.2 Aspettative ragionevoli degli interessati

35. Secondo il considerando 47, l'esistenza di un interesse legittimo richiede un'attenta valutazione. Qui il ragionevoli aspettative dell'interessato al momento e nel contesto del suo trattamento i dati personali devono essere inclusi. Per quanto riguarda il monitoraggio sistematico, la relazione tra i dati soggetto e responsabile del trattamento possono variare in modo significativo e influire sulle aspettative ragionevoli dei dati soggetto potrebbe avere. L'interpretazione del concetto di aspettative ragionevoli non dovrebbe essere solo

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

Pagina 11

basato sulle aspettative soggettive in questione. Piuttosto, il criterio decisivo deve essere se un obiettivo terzi potrebbero ragionevolmente aspettarsi e concludere di essere soggetti a monitoraggio in questa situazione specifica.

36. Ad esempio, nella maggior parte dei casi un dipendente nel suo posto di lavoro non si aspetta probabilmente di essere monitorato dal suo datore di lavoro. [12] Inoltre, non è previsto il monitoraggio nel proprio giardino privato, a zone giorno o in sale per esami e trattamenti. Allo stesso modo, non è ragionevole aspettarsi monitoraggio in strutture sanitarie o di sauna - il monitoraggio di tali aree è un'intensa intrusione nei diritti

dell'interessato. Le ragionevoli aspettative degli interessati sono che nessuna videosorveglianza lo farà si svolgono in quelle aree. D'altro canto, il cliente di una banca potrebbe aspettarsi di esserlo monitorato all'interno della banca o dal bancomat.

37. Le persone interessate possono anche aspettarsi di essere libere dal monitoraggio all'interno delle aree pubbliche, specialmente se pubbliche le aree sono in genere utilizzate per attività di recupero, rigenerazione e svago, nonché in luoghi in cui le persone soggiornano e / o comunicano, come aree salotto, tavoli in ristoranti, parchi, cinema e cinema strutture per il fitness. Qui gli interessi legittimi o i diritti e le libertà dell'interessato lo faranno spesso ignorare gli interessi legittimi del responsabile del trattamento.

Esempio: nei servizi igienici gli interessati si aspettano di non essere monitorati. Videosorveglianza per esempio prevenire incidenti non è proporzionale.

38.

39. I segni che informano il soggetto sulla videosorveglianza non hanno rilevanza nel determinare cosa a l'interessato può obiettivamente aspettarsi.

3.2 Necessità di eseguire un compito svolto nell'interesse pubblico o nell'esercizio di autorità ufficiale conferita al responsabile del trattamento, articolo 6, paragrafo 1, lettera e)

40. Se necessario, i dati personali potrebbero essere trattati mediante videosorveglianza ai sensi dell'articolo 6, paragrafo 1, lettera e) svolgere un compito svolto nell'interesse pubblico o nell'esercizio dell'autorità ufficiale. [13] Potrebbe essere che l'esercizio dell'autorità ufficiale non consente tale trattamento, ma altre basi legislative come "salute e sicurezza" per la protezione di dipendenti, visitatori e dipendenti possono fornire ambito di trattamento limitato, pur tenendo conto degli obblighi GDPR e dei diritti dell'interessato.

41. Gli Stati membri possono mantenere o introdurre specifiche normative nazionali per l'adattamento della videosorveglianza l'applicazione delle regole del GDPR determinando requisiti più precisi e specifici per elaborazione fintanto che è conforme ai principi stabiliti dal GDPR (ad es. conservazione limitazione, proporzionalità).

12 Vedi anche: Gruppo di lavoro articolo 29, parere 2/2017 sull'elaborazione dei dati sul lavoro, WP249, adottato l'8 giugno 2017.

13 Le basi del trattamento cui si fa riferimento sono stabilite dal diritto dell'Unione o dal diritto degli Stati membri » e «sono necessari per l'esecuzione di un compito svolto nell'interesse pubblico o nel esercizio dell'autorità ufficiale conferita al responsabile del trattamento (articolo 6, paragrafo 3).

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

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

43. Per quanto riguarda il monitoraggio sistematico, il consenso dell'interessato può solo servire da base giuridica in conformemente all'articolo 7 (cfr. considerando 43) in casi eccezionali. È nella natura della sorveglianza che questo la tecnologia controlla contemporaneamente un numero sconosciuto di persone. Il controller difficilmente sarà in grado di provare che l'interessato ha dato il proprio consenso prima del trattamento dei propri dati personali (articolo 7, paragrafo 1). Presunto che l'interessato revoca il proprio consenso, per il responsabile del trattamento sarà difficile dimostrarlo i dati non vengono più trattati (articolo 7, paragrafo 3).

Esempio: gli atleti possono richiedere il monitoraggio durante i singoli esercizi per analizzare il loro tecniche e prestazioni. D'altra parte, dove una società sportiva prende l'iniziativa monitorare un'intera squadra per lo stesso scopo, il consenso spesso non sarà valido, come l'individuo gli atleti possono sentirsi spinti a dare il consenso in modo che il loro rifiuto del consenso no influisce negativamente sui compagni di squadra.

44.

45. Se il responsabile del trattamento desidera fare affidamento sul consenso, è suo dovere assicurarsi che ogni persona interessata entri l'area sotto sorveglianza video ha dato il proprio consenso. Questo consenso deve soddisfare il condizioni dell'articolo 7. Accesso a un'area monitorata contrassegnata (ad es. le persone sono invitate ad attraversare a corridoio o cancello specifici per entrare in un'area monitorata), non costituisce una dichiarazione o un chiaro azione affermativa necessaria per il consenso, a meno che non soddisfi i criteri di cui agli articoli 4 e 7 come descritto nella linee guida sul consenso. [15]

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

47. La legislazione o gli accordi collettivi degli Stati membri, compresi gli "accordi di lavoro", possono prevedere disposizioni specifiche norme sul trattamento dei dati personali dei dipendenti nel contesto lavorativo (cfr. l'articolo 88).

4 COMUNICAZIONE DI VIDEO FOTOGRAFICO A TERZI

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

4.1 Divulgazione di riprese video a terzi in generale

49. La divulgazione è definita all'articolo 4, paragrafo 2, come trasmissione (ad es. Comunicazione individuale), diffusione (ad es. pubblicazione online) o messa a disposizione in altro modo. Le terze parti sono definite all'articolo 4, paragrafo 10. Dove la comunicazione è fatta a paesi terzi o organizzazioni internazionali, le disposizioni speciali dell'articolo 44 e seguenti si applicano anche.

14 Inoltre, il gruppo di lavoro articolo 29 (art. 29 WP) ha adottato "Linee guida sul consenso ai sensi dell'art Regolamento 2016/679 "(WP 259 rev. 01) che dovrebbe essere preso in considerazione.

15 Inoltre, il gruppo di lavoro ai sensi dell'articolo 29 (art. 29 WP) ha adottato "Linee guida sul consenso ai sensi dell'art Regolamento 2016/679 "(WP 259) che dovrebbe essere preso in considerazione.

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

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

51.

52. La trasmissione di riprese video a terzi per scopi diversi da quello per cui i dati è stato raccolto è possibile secondo le regole dell'articolo 6, paragrafo 4.

Esempio: la videosorveglianza di una barriera (in un parcheggio) è installata per risolvere danni. Si verifica un danno e la registrazione viene trasferita a un avvocato per perseguire un caso. In questo caso lo scopo per la registrazione è lo stesso di quello per il trasferimento.

Esempio: la videosorveglianza di una barriera (in un parcheggio) è installata per risolvere danni. La registrazione è pubblicata online per puro divertimento. In questo caso il lo scopo è cambiato e non è compatibile con lo scopo iniziale. Sarebbe inoltre problematico individuare una base giuridica per tale elaborazione (pubblicazione).

53.

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

4.2 Comunicazione di materiale video alle forze dell'ordine

55. La divulgazione di registrazioni video alle forze dell'ordine è anche un processo indipendente, che richiede una giustificazione separata per il controller.

56. Ai sensi dell'articolo 6, paragrafo 1, lettera c), il trattamento è legale se necessario per l'adempimento di un obbligo legale a cui è soggetto il responsabile del trattamento. Sebbene la legge di polizia applicabile sia una questione sotto il solo controllo degli Stati membri, esistono probabilmente regole generali che regolano il trasferimento di prove alla legge agenzie di contrasto in ogni stato membro. L'elaborazione del controller che consegna i dati è regolato dal GDPR. Se la legislazione nazionale impone al responsabile del trattamento di cooperare con la legge applicazione (es. indagine), la base giuridica per la consegna dei dati è un obbligo legale ai sensi Articolo 6, paragrafo 1, lettera c).

57. La limitazione delle finalità di cui all'articolo 6, paragrafo 4, è quindi spesso non problematica, poiché la divulgazione esplicitamente va ritorno alla legge degli Stati membri. Una considerazione dei requisiti speciali per un cambiamento di scopo nel senso di lit. a - e non è quindi necessario.

Esempio: un proprietario del negozio registra filmati alla sua entrata. Registra una persona che ruba un altro portafoglio della persona. La polizia chiede al responsabile del trattamento di consegnare il materiale per fornire assistenza la loro indagine. In tal caso il proprietario del negozio utilizzerà la base giuridica ai sensi dell'articolo 6, paragrafo 1, lettera c)

(obbligo legale) letto in combinato disposto con la legge nazionale pertinente per l'elaborazione del trasferimento.
Esempio: una videocamera è installata in un negozio per motivi di sicurezza. Il proprietario del negozio crede di averlo fatto
ha registrato qualcosa di sospetto nel suo filmato e decide di inviare il materiale alla polizia
(senza alcuna indicazione che siano in corso indagini di qualche tipo). In questo caso il
il proprietario del negozio deve valutare se sono soddisfatte le condizioni, nella maggior parte dei casi, dell'articolo 6, paragrafo 1, lettera f).

58.

59. Il trattamento dei dati personali da parte delle stesse forze dell'ordine non segue il
GDPR (vedi articolo 2, paragrafo 2, lettera d)), ma segue invece la direttiva sull'applicazione della legge (EU2016 / 680).

5 TRATTAMENTO DI CATEGORIE SPECIALI DI DATI

60. I sistemi di videosorveglianza di solito raccolgono enormi quantità di dati personali che possono rivelare dati di
una natura altamente personale e persino categorie speciali di dati. Anzi, dati apparentemente non significativi
originariamente raccolti tramite video possono essere utilizzati per dedurre altre informazioni per raggiungere uno scopo diverso
(ad es. per mappare le abitudini di un individuo). Tuttavia, la videosorveglianza non è sempre considerata come
trattamento di categorie speciali di dati personali.

Esempio: i filmati video che mostrano una persona interessata che indossa occhiali o usa una sedia a rotelle non lo sono
di per sé considerate categorie speciali di dati personali.

61.

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

2. Esempio: le opinioni politiche potrebbero ad esempio essere dedotte da immagini che mostrano identificabili
le persone interessate che partecipano a un evento, partecipano a uno sciopero, ecc. Ciò rientrerebbe nell'ambito di applicazione dell'articolo 9.

Esempio: un ospedale che installa una videocamera per monitorare le condizioni di salute di un paziente
sarebbe considerato come il trattamento di categorie speciali di dati personali (articolo 9).

63.

64. In linea di principio, in linea di principio, ogni volta che si installa un sistema di videosorveglianza dovrebbe essere attentamente considerata
essere dato al principio di minimizzazione dei dati. Pertanto, anche nei casi in cui non si applica l'articolo 9, paragrafo 1,
il responsabile del trattamento dei dati dovrebbe sempre cercare di ridurre al minimo il rischio di acquisire filmati rivelando altri sensibili
dati (oltre l'articolo 9), indipendentemente dall'obiettivo.

Esempio: la videosorveglianza che cattura una chiesa non rientra di per sé ai sensi dell'articolo 9. Tuttavia,
il responsabile del trattamento deve effettuare una valutazione particolarmente attenta ai sensi dell'articolo 6, paragrafo 1, lettera f), presa in considerazione
tenere conto della natura dei dati e del rischio di acquisire altri dati sensibili (oltre
Articolo 9) nella valutazione degli interessi dell'interessato.

65.

66. Se si utilizza un sistema di videosorveglianza per elaborare categorie speciali di dati, il responsabile del trattamento
deve identificare sia un'eccezione per l'elaborazione di categorie speciali di dati ai sensi dell'articolo 9 (ovvero
esenzione dalla regola generale che non si dovrebbero trattare categorie speciali di dati) e una legge
base ai sensi dell'articolo 6.

67. Ad esempio, l'articolo 9, paragrafo 2, lettera c) (il trattamento è necessario per proteggere gli interessi vitali dell'interessato
o di un'altra persona fisica in cui l'interessato non è fisicamente o legalmente in grado di fornire il consenso)
potrebbe - in teoria ed eccezionalmente - essere utilizzato, ma il responsabile del trattamento dei dati dovrebbe giustificarlo come un
assoluta necessità di salvaguardare gli interessi vitali di una persona e dimostrare che questa persona *"è fisicamente
o legalmente incapace di dare il proprio consenso "* . Inoltre, il titolare del trattamento non sarà autorizzato a utilizzare il
sistema per qualsiasi altro motivo.

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

68.

69. È importante notare qui che ogni esenzione elencata nell'articolo 9 non sarà probabilmente utilizzabile per giustificare trattamento di categorie speciali di dati attraverso la videosorveglianza. Più specificamente, i responsabili del trattamento dei dati il trattamento di tali dati nel contesto della videosorveglianza non può basarsi sull'articolo 9, paragrafo 2, lettera e), che consente trattamento relativo a dati personali manifestamente resi pubblici dall'interessato. Il semplice Il fatto di entrare nel raggio della telecamera non implica che l'interessato intenda effettuare categorie pubbliche speciali di dati che lo riguardano.

70. Inoltre, l'elaborazione di categorie speciali di dati richiede una vigilanza intensificata e costante a determinati obblighi; ad esempio un livello elevato di valutazione dell'impatto sulla sicurezza e sulla protezione dei dati dove necessario.

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

71.

5.1 Considerazioni generali sull'elaborazione di dati biometrici

72. L'uso di dati biometrici e in particolare il riconoscimento facciale comportano maggiori rischi per le persone interessate diritti. È fondamentale che il ricorso a tali tecnologie avvenga nel rispetto dei principi di liceità, necessità, proporzionalità e minimizzazione dei dati secondo quanto previsto dal GDPR. Considerando che l'uso di queste tecnologie possono essere percepite come particolarmente efficaci, i controllori dovrebbero prima di tutto valutare il impatto sui diritti e sulle libertà fondamentali e prendere in considerazione mezzi meno invasivi per raggiungerli finalità legittima del trattamento.

73. Per qualificarsi come dati biometrici come definito nel GDPR, elaborazione di dati grezzi, come quelli fisici, le caratteristiche fisiologiche o comportamentali di una persona fisica devono implicare una misurazione di ciò Caratteristiche. Poiché i dati biometrici sono il risultato di tali misurazioni, il GDPR afferma nel suo articolo 4.14 che è " *derivante da specifiche elaborazioni tecniche relative al fisico, fisiologico o caratteristiche comportamentali ".* Le riprese video di un individuo non possono tuttavia essere considerate di per sé come dati biometrici ai sensi dell'articolo 9, se non sono stati elaborati tecnicamente in modo specifico al fine di contribuire all'identificazione di un individuo. [16]

74. Per essere considerato un trattamento di categorie speciali di dati personali (articolo 9), è necessario che i dati biometrici siano elaborati "allo scopo di identificare in modo univoco una persona fisica".

75. In sintesi, alla luce degli articoli 4.14 e 9, devono essere considerati tre criteri:

- **Natura dei dati:** dati relativi alle caratteristiche fisiche, fisiologiche o comportamentali di a persona naturale,
- **Mezzi e modalità del trattamento** : dati "derivanti da un trattamento tecnico specifico",
- **Scopo del trattamento: i** dati devono essere utilizzati allo scopo di identificare in modo univoco un naturale persona.

76. L'uso della videosorveglianza inclusa la funzionalità di riconoscimento biometrico installata da privati le entità per i propri scopi (ad es. marketing, statistiche o persino di sicurezza), nella maggior parte dei casi, lo richiederanno

16 Il considerando 51 supporta questa analisi, affermando che " *l'elaborazione delle fotografie non dovrebbe sistematicamente essere considerato il trattamento di categorie speciali di dati personali così come sono coperti dalla definizione di dati biometrici solo se elaborati attraverso un mezzo tecnico specifico che lo consenta l'identificazione o l'autenticazione univoca di una persona fisica* ".

consenso esplicito di tutte le persone interessate (articolo 9, paragrafo 2, lettera a)), tuttavia un'altra eccezione adeguata all'articolo 9 potrebbe anche essere applicabile.

3. Esempio: per migliorare il proprio servizio, una società privata sostituisce il controllo di identificazione del passeggero punti 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 lo faranno hanno già dato il loro consenso esplicito e informato, dovranno arruolarsi per ad esempio un terminale automatico per creare e registrare il loro modello facciale associato con la carta d'imbarco e l'identità. I punti di controllo con riconoscimento facciale devono essere chiaramente separato, ad es. il sistema deve essere installato all'interno di un cavalletto in modo che i modelli biometrici di la persona non consenziente non verrà catturata. Solo i passeggeri, che avranno in precedenza dato il loro consenso e proceduto alla loro iscrizione, utilizzerà il cavalletto dotato di sistema biometrico.

4. Esempio: un controller gestisce l'accesso al suo edificio utilizzando un metodo di riconoscimento facciale. Persone possono utilizzare questo modo di accesso solo se hanno dato il loro consenso esplicitamente informato (secondo

all'articolo 9, paragrafo 2, lettera a)) in anticipo. Tuttavia, al fine di garantire che nessuno che non ha precedentemente dato il consenso acquisito, il metodo di riconoscimento facciale dovrebbe essere attivato da l'interessato stesso, ad esempio premendo un pulsante. Per garantire la liceità del elaborazione, il controller deve sempre offrire un modo alternativo per accedere all'edificio, senza elaborazione biometrica, come badge o chiavi.

77.

78. In questo tipo di casi, in cui vengono generati modelli biometrici, i controllori devono assicurarsi che una volta a è stato ottenuto il risultato di match o no-match, tutti i template intermedi realizzati al volo (con il consenso esplicito e informato dell'interessato) al fine di essere confrontato con quelli creati dall'interessato gli interessati al momento dell'arruolamento, vengono immediatamente e in modo sicuro cancellati. I modelli creato per l'arruolamento dovrebbe essere conservato solo per la realizzazione dello scopo del trattamento e non deve essere archiviato o archiviato.

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

5. Esempio: il proprietario di un negozio desidera personalizzare la propria pubblicità in base al sesso e all'età caratteristiche del cliente catturate da un sistema di videosorveglianza. In caso contrario generare modelli biometrici al fine di identificare in modo univoco le persone, ma invece rileva solo quelle caratteristiche fisiche e di conseguenza classifica solo la persona, quindi l'elaborazione non rientrerebbe nell'articolo 9.

80.

81. Tuttavia, l'articolo 9 si applica se il responsabile del trattamento memorizza i dati biometrici (più comunemente tramite modelli che sono creati dall'estrazione di caratteristiche chiave dalla forma grezza di dati biometrici (ad es. viso misurazioni da un'immagine)) per identificare in modo univoco una persona. Se un controller desidera rilevare una persona interessata che rientra nell'area o che entra in un'altra area (ad esempio per continuare il progetto pubblicità personalizzata), lo scopo sarebbe quindi quello di identificare in modo univoco una persona fisica, ovvero che l'operazione ricadrebbe dall'inizio ai sensi dell'articolo 9. Ciò potrebbe accadere se un controllore memorizza modelli generati per fornire ulteriori annunci pubblicitari su più cartelloni pubblicitari in tutto diverse posizioni all'interno del negozio. Dal momento che il sistema utilizza caratteristiche fisiche per rilevare specifici individui che rientrano nel raggio di azione della videocamera (come i visitatori di un centro commerciale) e che seguono

Pagina 17

essi costituirebbero un metodo di identificazione biometrica perché è finalizzato al riconoscimento attraverso l'uso di elaborazioni tecniche specifiche.

6. Esempio: un proprietario del negozio ha installato un sistema di riconoscimento facciale all'interno del suo negozio per farlo personalizzare la sua pubblicità verso gli individui. Il titolare del trattamento deve ottenere l'esplicito e il consenso informato di tutti gli interessati prima di utilizzare questo sistema biometrico e fornire pubblicità su misura. Il sistema sarebbe illegale se cattura visitatori o passanti da chi non hanno acconsentito alla creazione del loro modello biometrico, anche se il loro modello è stato eliminato entro il periodo più breve possibile. In effetti, questi modelli temporanei costituiscono biometrici dati trattati al fine di identificare in modo univoco una persona che potrebbe non voler ricevere targetizzati annuncio pubblicitario.

82.

83. L'EDPB osserva che alcuni sistemi biometrici sono installati in un ambiente non controllato [17] , che significa che il sistema prevede di catturare al volo le facce di ogni individuo che passa nel raggio di la videocamera, comprese le persone che non hanno acconsentito al dispositivo biometrico, creando così modelli biometrici. Questi modelli vengono confrontati con quelli creati dagli interessati il loro consenso preventivo durante un processo di arruolamento (ad es. un utente di dispositivi biometrici) per i dati controller per riconoscere se la persona è un utente del dispositivo biometrico o meno. In questo caso, il sistema è spesso progettato per discriminare le persone che vuole riconoscere da un database da coloro che non sono arruolati. Poiché lo scopo è identificare in modo univoco le persone fisiche, un'eccezione ai sensi dell'articolo 9 (2) GDPR è ancora necessario per chiunque sia stato catturato dalla fotocamera.

7. Esempio: un hotel utilizza la videosorveglianza per avvisare automaticamente il direttore dell'hotel di un VIP arrivato quando viene riconosciuto il volto dell'ospite. Questi VIP hanno già dato il loro esplicito acconsenti all'uso del riconoscimento facciale prima di essere registrato in un database istituito per questo scopo. Questi sistemi di trattamento dei dati biometrici sarebbero illegali a meno che tutti gli altri ospiti monitorati (al fine di identificare i VIP) hanno acconsentito al trattamento ai sensi dell'articolo 9 (2) (a) GDPR.

8. Esempio: un controller installa un sistema di videosorveglianza con riconoscimento facciale all'ingresso della sala da concerto che gestisce. Il responsabile del trattamento deve impostare ingressi chiaramente separati; uno con un sistema biometrico e uno senza (dove invece ad esempio scansiona un biglietto). Il gli ingressi dotati di dispositivi biometrici devono essere installati e resi accessibili in un certo modo

ciò impedisce al sistema di acquisire modelli biometrici di spettatori non consenzienti.

84.

85. Infine, quando il consenso è richiesto dall'articolo 9 del GDPR, il responsabile del trattamento dei dati non deve condizionare il accesso ai suoi servizi all'accettazione del trattamento biometrico. In altre parole e in particolare quando il trattamento biometrico viene utilizzato a scopo di autenticazione, il titolare del trattamento deve offrire un soluzione alternativa che non prevede l'elaborazione biometrica - senza vincoli o costi aggiuntivi per l'interessato. Questa soluzione alternativa è necessaria anche per le persone che non soddisfano il vincoli del dispositivo biometrico (impossibile registrare o leggere i dati biometrici, disabilità situazione che ne rende difficile l'utilizzo, ecc.) e in previsione di indisponibilità del dispositivo biometrico

17 Significa che il dispositivo biometrico si trova in uno spazio aperto al pubblico ed è in grado di lavorare chiunque passi, al contrario dei sistemi biometrici in ambienti controllati che possono essere utilizzati solo accettando la partecipazione della persona.

(come un malfunzionamento del dispositivo), è necessario implementare una "soluzione di backup" per garantire la continuità del servizio proposto, limitato tuttavia a un uso eccezionale.

5.2 Misure suggerite per ridurre al minimo i rischi durante l'elaborazione dei dati biometrici

86. In conformità con il principio di minimizzazione dei dati, i responsabili del trattamento dei dati devono garantire che i dati estratti da un'immagine digitale per costruire un modello non sarà eccessivo e conterrà solo le informazioni richiesto per lo scopo specificato, evitando così ogni possibile ulteriore elaborazione. Le misure dovrebbero essere messo in atto per garantire che i modelli non possano essere trasferiti attraverso sistemi biometrici.

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

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

89. Inoltre, i responsabili del trattamento dei dati devono procedere alla cancellazione dei dati non elaborati (immagini dei volti, segnali vocali, ecc andatura, ecc.) e garantire l'efficacia di questa cancellazione. In effetti, nella misura in cui derivano i modelli biometrici da tali dati, si può considerare che la costituzione di basi di dati potrebbe rappresentare un uguale se no minaccia ancora più grande (perché potrebbe non essere sempre facile leggere un modello biometrico senza il conoscenza di come è stato programmato, mentre i dati grezzi saranno la base di qualsiasi modello). Nel caso in cui il responsabile del trattamento dei dati debba conservare tali dati, metodo di aggiunta del rumore (come filigrana), che renderebbe inefficace la creazione del modello. Il il responsabile del trattamento deve anche eliminare dati e modelli biometrici in caso di accesso non autorizzato a leggere il confronto comparativo o il server di archiviazione ed eliminare tutti i dati non utili per ulteriori elaborazioni su la fine della vita del dispositivo biometrico.

6 DIRITTI DEL SOGGETTO DATI

90. A causa del carattere del trattamento dei dati quando si utilizza la videosorveglianza, alcuni diritti dell'interessato sono soggetti a Il GDPR serve ulteriori chiarimenti. Questo capitolo non è tuttavia esaustivo, tutti i diritti previsti dal GDPR si applica al trattamento dei dati personali attraverso la videosorveglianza.

6.1 Diritto di accesso

91. L'interessato ha diritto di ottenere la conferma dal responsabile del trattamento in merito alla sua o meno i dati personali sono in fase di elaborazione. Per la videosorveglianza ciò significa che se non vengono archiviati dati o trasferito in qualsiasi modo, una volta trascorso il momento di monitoraggio in tempo reale, il controller potrebbe farlo fornire solo l'informazione che non vengono più elaborati dati personali (oltre al generale

Pagina 19

obblighi di informazione ai sensi dell'articolo 13, cfr. *sezione 7 - Trasparenza e obblighi di informazione*). Se tuttavia i dati vengono ancora elaborati al momento della richiesta (ovvero se i dati vengono archiviati o in modo continuo trattati in altro modo), l'interessato dovrebbe ricevere accesso e informazioni in conformità con l'articolo 15.

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

L'articolo 15, paragrafo 4, del GDPR, incide negativamente sui diritti degli altri

93. Detto questo, qualsiasi numero di persone interessate può essere registrato nella stessa sequenza di videosorveglianza uno screening provocherebbe quindi un trattamento aggiuntivo dei dati personali di altri interessati. Se i dati soggetto desidera ricevere una copia del materiale (articolo 15, paragrafo 3), ciò potrebbe influire negativamente sui diritti e le libertà di altri interessati nel materiale. Per evitare tale effetto, il controller dovrebbe pertanto prendere in considerazione che a causa della natura intrusiva del filmato il controller in alcuni casi non dovrebbe distribuire filmati in cui è possibile identificare altri soggetti. Il la protezione dei diritti di terzi non dovrebbe tuttavia essere utilizzata come scusa per impedire il legittimo richieste di accesso da parte di individui, il responsabile del trattamento dovrebbe invece implementare misure tecniche da soddisfare la richiesta di accesso (ad esempio, modifica delle immagini come mascheramento o rimescolamento).

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

94. Se il filmato non è ricercabile per i dati personali, (probabilmente il controller avrebbe per esaminare una grande quantità di materiale immagazzinato al fine di trovare l'interessato in questione) il responsabile del trattamento potrebbe non essere in grado di identificare l'interessato.

95. Per questi motivi l'interessato dovrebbe (oltre a identificarsi anche con l'identificazione documento o di persona) nella sua richiesta al responsabile del trattamento, specificare quando - entro un termine ragionevole in proporzione alla quantità di soggetti registrati - è entrato nell'area monitorata. Il il responsabile del trattamento deve informare preventivamente l'interessato in merito alle informazioni necessarie per il responsabile del trattamento per soddisfare la richiesta. Se il controller è in grado di dimostrare che non è in una posizione per identificare l'interessato, il responsabile del trattamento deve informare l'interessato di conseguenza, se possibile.

Esempio: se l'interessato richiede una copia dei propri dati personali trattati videosorveglianza all'ingresso di un centro commerciale con 30.000 visitatori al giorno, i dati il soggetto deve specificare quando ha superato l'area monitorata entro circa due- ora-temporale. Se il controller elabora ancora il materiale una copia del filmato dovrebbe essere fornito. Se altri interessati possono essere identificati nello stesso materiale, allora quello parte del materiale deve essere anonimizzata (ad esempio sfocando la copia o parti di essa) prima di consegnare la copia all'interessato che ha presentato la richiesta.

Esempio: se il controller cancella automaticamente tutte le riprese, ad esempio entro 2 giorni, un dato il soggetto può accedere solo a tali informazioni [che il materiale è stato eliminato] se la richiesta viene presentata al controller post quei 2 giorni.

96.

Articolo 12 GDPR, richieste eccessive

97. In caso di richieste eccessive o manifestamente infondate da una persona interessata, il responsabile del trattamento può addebitare una commissione ragionevole ai sensi dell'articolo 12, paragrafo 5, lettera a), del GDPR, oppure rifiutare di agire in base al richiesta (articolo 12, paragrafo 5, lettera b), del regolamento generale sulla protezione dei dati. Il responsabile del trattamento deve essere in grado di dimostrare l'eccessivo o carattere manifestamente infondato della richiesta.

Pagina 20

6.2 Diritto alla cancellazione e diritto di opposizione

6.2.1 Diritto alla cancellazione (diritto all'oblio)

98. Se il responsabile del trattamento continua a elaborare i dati personali oltre il monitoraggio in tempo reale (ad es. Memorizzazione) dei dati il soggetto può richiedere la cancellazione dei dati personali ai sensi dell'articolo 17 GDPR.

99. Su richiesta, il responsabile del trattamento è tenuto a cancellare i dati personali senza indebito ritardo se uno dei circostanze elencate ai sensi dell'articolo 17, paragrafo 1, del GDPR (e nessuna delle eccezioni elencate ai sensi dell'articolo 17 (3) GDPR lo fa). Ciò include 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 illegale (vedi anche

sezione 8 relativa ai periodi di conservazione e all'obbligo di cancellazione). Inoltre, a seconda della base giuridica di il trattamento, i dati personali devono essere cancellati:

- *per il consenso* ogni volta che il consenso viene revocato (e non esiste altra base giuridica per il in lavorazione)
- per legittimo interesse:
  - ogni volta che l'interessato esercita il diritto di opposizione (vedere la *sezione 6.2.2*) e lì non sono motivi legittimi convincenti imperativi per l'elaborazione, o
  - in caso di marketing diretto (compresa la profilazione) ogni volta che l'interessato si oppone l'elaborazione.

100. Se il responsabile del trattamento ha reso pubbliche le riprese video (ad es. Trasmissione o streaming online), ragionevole è necessario adottare delle misure per informare gli altri responsabili del trattamento (che ora stanno elaborando i dati personali in questione) della richiesta ai sensi dell'articolo 17, paragrafo 2, del GDPR. I passaggi ragionevoli dovrebbero includere misure tecniche, tenendo conto della tecnologia disponibile e dei costi di attuazione. Al per quanto possibile, il responsabile del trattamento dovrebbe informare - in caso di cancellazione dei dati personali - chiunque a cui il i dati personali precedentemente sono stati divulgati, ai sensi dell'articolo 19 del GDPR.

101. Oltre all'obbligo del responsabile del trattamento di cancellare i dati personali su richiesta dell'interessato, il il responsabile del trattamento è tenuto ai sensi dei principi generali del GDPR di limitare i dati personali memorizzati (vedere *sezione 8)* .

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

Esempio: un negozio di alimentari ha problemi di vandalismo, in particolare all'esterno e utilizza pertanto la videosorveglianza al di fuori del loro ingresso in collegamento diretto con il muri. Un passante chiede di cancellare i suoi dati personali da quel momento. Il il responsabile del trattamento è tenuto a rispondere alla richiesta senza indebito ritardo e al più tardi entro un mese. Dal momento che il filmato in questione non soddisfa più lo scopo per cui era inizialmente memorizzato (non si sono verificati atti di vandalismo durante il periodo in cui l'interessato è passato) il momento della richiesta, nessun interesse legittimo per archiviare i dati che sovrascriverebbero interessi degli interessati. Il responsabile del trattamento deve cancellare i dati personali.

103.

6.2.2 Diritto di opposizione

104. Per la videosorveglianza basata sull'interesse *legittimo* (Articolo 6 (1) (f) GDPR) o per la necessità quando svolgere un compito di *interesse pubblico* (articolo 6, paragrafo 1, lettera e), del GDPR) l'interessato ha diritto - in qualsiasi tempo - di opporsi, per motivi relativi alla sua situazione particolare, al trattamento in conformità

con l'articolo 21 del GDPR. A meno che il responsabile del trattamento non dimostri validi motivi legittimi che prevalgono i diritti e gli interessi della persona interessata, il trattamento dei dati della persona che ha obiettato deve poi fermati. Il responsabile del trattamento dovrebbe essere tenuto a rispondere alle richieste dell'interessato senza indebito ritardo e al più tardi entro un mese.

105. Nel contesto della videosorveglianza, questa obiezione potrebbe essere sollevata prima di entrare, durante il tempo all'interno o dopo aver lasciato l'area monitorata. In pratica ciò significa che, a meno che il controller non lo abbia convincenti motivi legittimi, il monitoraggio di un'area in cui le persone fisiche potrebbero essere identificate è solo lecito se uno dei due

(1) il controller è in grado di fermare immediatamente la fotocamera dal trattamento dei dati personali quando richiesto, o

(2) l'area monitorata è così limitata nei dettagli in modo che il responsabile del trattamento possa garantire l'approvazione dall'interessato prima di entrare nell'area e non è un'area che l'interessato come a il cittadino ha diritto all'accesso.

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

Esempio: un'azienda sta riscontrando difficoltà con violazioni della sicurezza all'ingresso pubblico e utilizza la videosorveglianza per motivi di legittimo interesse, al fine di catturare coloro che entrano illegalmente. Un visitatore si oppone al trattamento dei propri dati attraverso il sistema di videosorveglianza per motivi relativi alla sua situazione particolare. Il la società tuttavia in questo caso rifiuta la richiesta con la spiegazione che il filmato è necessario archiviato a causa di un'indagine interna in corso, quindi convincente motivi legittimi per continuare il trattamento dei dati personali.

107.

7 OBBLIGHI DI TRASPARENZA E INFORMAZIONE [18]

108. È da tempo inerente alla legislazione europea sulla protezione dei dati che gli interessati dovrebbero essere a conoscenza del fatto che la videosorveglianza è in funzione. Dovrebbero essere informati in modo dettagliato in merito al luoghi monitorati. [19] Ai sensi del GDPR sono stabiliti obblighi generali di trasparenza e informazione nell'articolo 12 del GDPR e seguenti. Linee guida del gruppo di lavoro "Articolo 29" sulla trasparenza ai sensi del regolamento 2016/679 (WP260)"che sono state approvate dal EDPB il 25 maggio ◦ 2018 forniscono ulteriori dettagli. Nel linea con WP260 para. 26, è l'articolo 13 del GDPR, applicabile se i dati personali sono raccolti "da una persona interessata per osservazione (ad esempio utilizzando dispositivi di acquisizione dati automatizzati o software di acquisizione dati come le telecamere) ".

109. Alla luce del volume di informazioni, che è necessario fornire all'interessato, un livello l'approccio può essere seguito dai responsabili del trattamento dei dati laddove decidano di utilizzare una combinazione di metodi assicurare la trasparenza (WP260, par. 35; WP89, p. 22). Per quanto riguarda la videosorveglianza, la più importante

18 Potrebbero essere applicati requisiti specifici nella legislazione nazionale.

19 Gruppo di lavoro articolo 29, parere 4/2004 sul trattamento dei dati personali mediante video Sorveglianza (WP89).

le informazioni dovrebbero essere visualizzate sul segnale di avvertimento stesso (primo strato) mentre le ulteriori obbligatorie i dettagli possono essere forniti con altri mezzi (secondo strato).

7.1 Informazioni sul primo strato (segnale di avvertimento)

110. Il primo livello riguarda il modo principale in cui il responsabile del trattamento si impegna per la prima volta con l'interessato. A in questa fase, i controller possono utilizzare un segnale di avvertimento che mostra le informazioni pertinenti. Il visualizzato le informazioni possono essere fornite in combinazione con un'icona al fine di fornire, in modo facilmente visibile, modo comprensibile e chiaramente leggibile, una panoramica significativa del trattamento previsto (articolo 12 (7) GDPR). Il formato delle informazioni dovrebbe essere adattato alla posizione individuale (WP89 p. 22).

7.1.1 Posizionamento del segnale di avvertimento

111. Le informazioni dovrebbero essere posizionate a una distanza ragionevole dai luoghi monitorati (WP 89, p. 22) in modo tale che l'interessato possa facilmente riconoscere prima le circostanze della sorveglianza entrare nell'area monitorata (approssimativamente all'altezza degli occhi). Non è necessario specificare l'esatto posizione dell'apparecchiatura di sorveglianza purché non vi siano dubbi, a quali aree sono soggette il monitoraggio e il contesto della sorveglianza devono essere chiariti in modo inequivocabile (WP 89, p. 22). I dati il soggetto deve essere in grado di stimare quale area è catturata da una fotocamera in modo che sia in grado di evitare sorveglianza o adeguare il suo comportamento, se necessario.

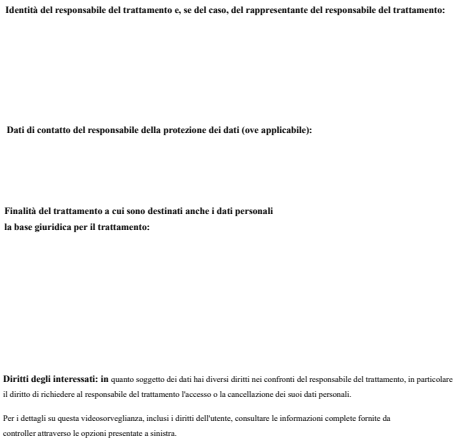
7.1.2 Contenuto del primo livello

112. Le informazioni del primo strato (segnale di avvertimento) dovrebbero in genere trasmettere le informazioni più importanti, ad es i dettagli delle finalità del trattamento, l'identità del responsabile del trattamento e l'esistenza dei diritti di l'interessato, unitamente alle informazioni sui maggiori impatti del trattamento. [20] Questo può includere ad esempio gli interessi legittimi perseguiti dal responsabile del trattamento (o da una terza parte) e contattare dettagli del responsabile della protezione dei dati (se applicabile). Deve anche fare riferimento al secondo più dettagliato strato di informazioni e dove e come trovarlo.

113. Inoltre, il segno dovrebbe contenere anche tutte le informazioni che potrebbero sorprendere l'interessato (WP260, par. 38). Ciò potrebbe ad esempio essere trasmissioni a terzi, in particolare se localizzati al di fuori dell'UE e il periodo di conservazione. Se queste informazioni non sono indicate, l'interessato dovrebbe esserlo in grado di fidarsi che esiste solo un monitoraggio dal vivo (senza alcuna registrazione o trasmissione di dati a terzi parti).

20 Vedi WP260, par. 38

Esempio:



114.

7.2 Informazioni sul secondo livello

115. Le informazioni di secondo livello devono anche essere rese disponibili in un luogo facilmente accessibile ai dati soggetto, ad esempio come un foglio informativo completo disponibile in una posizione centrale (ad es. informazioni scrivania, reception o cassiere) o visualizzati su un poster facilmente accessibile. Come accennato in precedenza, il primo il segnale di avvertimento del livello deve riferirsi chiaramente alle informazioni del secondo livello. Inoltre, è meglio se il primo le informazioni sul livello si riferiscono a una fonte digitale (ad es. codice QR o indirizzo di un sito Web) del secondo livello. Tuttavia, le informazioni dovrebbero anche essere facilmente disponibili in modo non digitale. In ogni caso, deve essere possibile per accedere alle informazioni del secondo livello senza entrare nell'area rilevata. Questo può essere raggiunto per esempio da un collegamento o qualsiasi altro mezzo appropriato come un numero di telefono che può essere chiamato. Deve contenere tutte le altre informazioni obbligatorie ai sensi dell'articolo 13 del GDPR.

116. Oltre a queste opzioni e anche per renderle più efficaci, l'EDPB promuove l'uso di mezzi tecnologici per fornire informazioni agli interessati. Ciò può includere ad esempio; geolocalizzazione telecamere e includendo informazioni nella mappatura di app o siti Web in modo che le persone possano farlo facilmente, da un lato, identificare e specificare le fonti video relative all'esercizio dei loro diritti, e, d'altra parte, ottenere informazioni più dettagliate sull'operazione di elaborazione.

Esempio: un proprietario di un negozio sta monitorando il suo negozio. Per conformarsi all'articolo 13 è sufficiente posizionare un segnale di avvertimento in un punto facilmente visibile all'ingresso del suo negozio, che contiene il file informazioni di primo livello. Inoltre, deve fornire una scheda contenente il informazioni di secondo livello presso la cassa o qualsiasi altra posizione centrale e facilmente accessibile nella sua negozio.

117.

8 PERIODI DI CONSERVAZIONE E OBBLIGO DI CANCELLAZIONE

118. I dati personali non possono essere conservati più a lungo di quanto necessario per le finalità per le quali il personale
i dati vengono elaborati (articolo 5, paragrafo 1, lettere c) ed e) GDPR). In alcuni stati membri, potrebbero esserci specifici
disposizioni relative ai periodi di conservazione per quanto riguarda la videosorveglianza ai sensi dell'articolo 6, paragrafo 2, del GDPR.

119. Se i dati personali sono necessari per l'archiviazione o meno, dovrebbero essere controllati entro una tempistica ristretta.
In generale, scopi legittimi per la videosorveglianza sono spesso la protezione o la conservazione della proprietà
prova. Di solito i danni che si sono verificati possono essere riconosciuti entro uno o due giorni. Prendere parte in
considerare i principi dell'articolo 5, paragrafo 1, lettere c) ed e), del GDPR, vale a dire la minimizzazione e la conservazione dei dati
limitazione, i dati personali dovrebbero essere nella maggior parte dei casi (ad esempio allo scopo di rilevare atti di vandalismo)
cancellato, idealmente automaticamente, dopo alcuni giorni. Più è impostato il periodo di archiviazione (soprattutto quando
oltre 72 ore), maggiore è l'argomentazione per la legittimità dello scopo e la necessità di
lo stoccaggio deve essere fornito. Se il controller utilizza la videosorveglianza non solo per monitorare i propri locali
ma intende anche archiviare i dati, il controller deve assicurare che l'archiviazione sia effettivamente necessaria
per raggiungere lo scopo. In tal caso, il periodo di conservazione deve essere chiaramente definito e impostato individualmente
per ogni scopo particolare. È responsabilità del responsabile del trattamento definire il periodo di conservazione in
conformità con i principi di necessità e proporzionalità e per dimostrare la conformità
le disposizioni del GDPR.

Esempio: un proprietario di un piccolo negozio normalmente si accorgerebbe di qualsiasi vandalismo uguale
giorno. Di conseguenza, è sufficiente un periodo di conservazione regolare di 24 ore. Fine settimana chiuso o
le festività potrebbero tuttavia essere motivi per un periodo di conservazione più lungo. Se viene rilevato un danno lui
potrebbe anche essere necessario archiviare il filmato per un periodo più lungo al fine di intraprendere un'azione legale contro
l'autore del reato.

120.

9 MISURE TECNICHE E ORGANIZZATIVE

121. Come indicato nell'articolo 32, paragrafo 1, del GDPR, il trattamento dei dati personali durante la videosorveglianza non deve solo
essere legalmente consentito, ma anche i controllori e i processori devono garantirlo adeguatamente. implementato
le misure organizzative e tecniche devono essere **proporzionali ai rischi per i diritti e le libertà di**
persone fisiche , risultanti da distruzione accidentale o illegale, perdita, alterazione, non autorizzata
divulgazione o accesso ai dati di videosorveglianza. Ai sensi degli articoli 24 e 25 del GDPR, i responsabili del trattamento hanno bisogno
attuare misure tecniche e organizzative anche al fine di salvaguardare tutta la protezione dei dati
principi durante il trattamento e stabilire i mezzi affinché gli interessati possano esercitare i loro diritti come definiti
negli articoli 15-22 GDPR. I responsabili del trattamento dei dati dovrebbero adottare un quadro interno e politiche che garantiscano
questa implementazione sia al momento della determinazione dei mezzi per l'elaborazione che al momento
del trattamento stesso, compresa l'esecuzione delle valutazioni di impatto sulla protezione dei dati quando
necessario.

9.1 Panoramica del sistema di videosorveglianza

Un sistema di videosorveglianza (VSS) 21 è composto da dispositivi analogici e digitali e da software per il
lo scopo di catturare immagini di una scena, gestirle e mostrarle a un operatore. Suo
i componenti sono raggruppati nelle seguenti categorie:

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

- lo scopo dell'acquisizione di immagini è la generazione di un'immagine del mondo reale in tale ambito
  formato che può essere utilizzato dal resto del sistema
- `le` interconnessioni descrivono tutta la trasmissione di dati all'interno dell'ambiente video, ad es
  connessioni e comunicazioni. Esempi di collegamenti sono cavi, digitali
  reti e trasmissioni wireless. Le comunicazioni descrivono tutto il video e il controllo
  segnali di dati, che potrebbero essere digitali o analogici
- `la` gestione delle immagini include 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, incluso l'operatore di gestione
  comandi e attività generate dal sistema (procedure di allarme, operatori di allerta)

- le interfacce con altri sistemi potrebbero includere la connessione ad altri sistemi di sicurezza (controllo degli accessi, allarme antincendio) e sistemi non di sicurezza (sistemi di gestione dell'edificio, automatici riconoscimento della targa)

La sicurezza VSS consiste nella riservatezza, integrità e disponibilità del sistema e dei dati

- la sicurezza del sistema include la sicurezza fisica di tutti i componenti del sistema e il controllo di accesso al VSS
- la sicurezza dei dati include la prevenzione della perdita o della manipolazione dei dati

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

122.

Figura 1- Sistema di videosorveglianza

9.2 Protezione dei dati in base alla progettazione e per impostazione predefinita

123. Come indicato nell'articolo 25 del GDPR, i responsabili del trattamento devono attuare un'adeguata protezione dei dati tecnici e misure organizzative non appena pianificano la videosorveglianza, prima di iniziare la raccolta ed elaborazione di filmati video. Questi principi sottolineano la necessità di migliorare la privacy integrata tecnologie, impostazioni predefinite che riducono al minimo l'elaborazione dei dati e la fornitura del necessario strumenti che consentono la massima protezione possibile dei dati personali [22] .

124. I responsabili del trattamento dovrebbero integrare la protezione dei dati e la tutela della privacy non solo nelle specifiche di progettazione della tecnologia ma anche nelle pratiche organizzative. Quando si tratta di pratiche organizzative, il il responsabile del trattamento dovrebbe adottare un quadro di gestione adeguato, stabilire e applicare politiche e procedure relative alla videosorveglianza. Dal punto di vista tecnico, specifiche di sistema e la progettazione dovrebbe includere i requisiti per il trattamento dei dati personali secondo i principi indicati nell'articolo 5 GDPR (liceità del trattamento, finalità e limitazione dei dati, minimizzazione dei dati per impostazione predefinita ai sensi dell'articolo 25, paragrafo 2, del GDPR, integrità e riservatezza, responsabilità ecc.). Nel caso in cui un controller prevede di acquisire un sistema di videosorveglianza commerciale, il controllore deve includerli requisiti nelle specifiche di acquisto. Il responsabile del trattamento deve garantire la conformità con questi requisiti che li applicano a tutti i componenti del sistema e a tutti i dati elaborati da esso, durante il loro intero ciclo di vita.

9.3 Esempi concreti di misure pertinenti

125. La maggior parte delle misure che possono essere utilizzate per proteggere la videosorveglianza, specialmente quando si utilizzano apparecchiature digitali e vengono utilizzati software, non differiranno da quelli utilizzati in altri sistemi IT. Tuttavia, indipendentemente dal soluzione selezionata, il controller deve proteggere adeguatamente tutti i componenti di una videosorveglianza

22 Parere 168 del WP sul tema "Il futuro della privacy", contributo congiunto dei dati dell'articolo 29 Gruppo di lavoro sulla protezione e gruppo di lavoro sulla polizia e la giustizia alla consultazione del Commissione europea sul quadro giuridico per il diritto fondamentale alla protezione delle persone dati (adottato il 01 dicembre 2009), https://ec.europa.eu/justice/Article-29 / documentazione / opinione-raccomandazione / files / 2009 / wp168_en.pdf

Pagina 27

sistema e dati in tutte le fasi, vale a dire durante la memorizzazione (dati a riposo), la trasmissione (dati in transito) e elaborazione (dati in uso). Per questo, è necessario che controller e processori combinino l'organizzazione e misure tecniche.

126. Nella scelta delle soluzioni tecniche, il responsabile del trattamento dovrebbe considerare anche le tecnologie rispettose della privacy perché migliorano la sicurezza. Esempi di tali tecnologie sono i sistemi che consentono il mascheramento o aree di confusione non rilevanti per la sorveglianza o la modifica di immagini di terze persone, quando si forniscono riprese video agli interessati. [23] D'altra parte, le soluzioni selezionate non dovrebbero fornire funzioni non necessarie (ad es. movimento illimitato di telecamere, capacità di zoom, radio trasmissione, analisi e registrazioni audio). Le funzioni fornite, ma non necessarie, devono essere disattivato.

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

9.3.1 Misure organizzative

128. A parte una potenziale DPIA necessaria (vedere la sezione 10), i responsabili del trattamento dovrebbero considerare i seguenti argomenti quando creano le proprie politiche e procedure di videosorveglianza:

- Chi è responsabile della gestione e del funzionamento del sistema di videosorveglianza
- Scopo e portata del progetto di videosorveglianza
- Uso appropriato e proibito (dove e quando è consentita la videosorveglianza e dove e quando non lo è; ad es. uso di telecamere nascoste e audio oltre 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, incluso l'archiviazione delle registrazioni video in relazione a 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 incidente di violazione dei dati)
- Quali procedure devono seguire le parti esterne per richiedere le registrazioni video e procedure per rifiutare o accogliere tali richieste
- Procedure per l'approvvigionamento, l'installazione e la manutenzione di VSS
- Procedure di gestione e recupero degli incidenti.

23 L'uso di tali tecnologie può anche essere obbligatorio in alcuni casi per conformarsi all'articolo 5 (1) (c). In ogni caso possono servire come esempi di buone pratiche.

24 IEC TS 62045 - Sicurezza multimediale - Linee guida per la protezione della privacy di apparecchiature e sistemi in 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

9.3.2 Misure tecniche

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

130. **La sicurezza fisica** è una parte vitale della protezione dei dati e la prima linea di difesa, perché protegge VSS equipaggiamento da furto, vandalismo, calamità naturale, catastrofi provocate dall'uomo e danni accidentali (ad es. da sovratensioni elettriche, temperature estreme e caffè versato). Nel caso di un analogo basato sistemi, la sicurezza fisica svolge il ruolo principale nella loro protezione.

131. **Sicurezza del sistema e dei dati,** vale a dire protezione contro interferenze intenzionali e non intenzionali le normali operazioni possono includere:

- Protezione dell'intera infrastruttura VSS (comprese telecamere remote, cavi e alimentazione fornitura) contro manomissioni fisiche e furti
- Protezione della trasmissione di filmati con canali di comunicazione sicuri contro l'intercettazione
- Crittografia dei dati
- Utilizzo di soluzioni basate su hardware e software come firewall, antivirus o intrusioni sistemi di rilevamento contro attacchi informatici
- Rilevamento di guasti di componenti, software e interconnessioni
- Mezzi per ripristinare la disponibilità e l'accesso al sistema in caso di problemi fisici o tecnici incidente.

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

- Garantire che tutti i locali in cui viene effettuato il monitoraggio della videosorveglianza e delle riprese video archiviati sono protetti contro l'accesso non supervisionato da parte di terzi
- Posizionamento dei monitor in modo tale (specialmente quando si trovano in aree aperte, come una reception) in modo che solo gli operatori autorizzati possano visualizzarli
- Sono definite e procedure per la concessione, modifica e revoca dell'accesso fisico e logico forzata.
- Metodi e mezzi di autenticazione e autorizzazione dell'utente, ad esempio lunghezza delle password e la frequenza di cambiamento sono implementate.
- Le azioni eseguite dall'utente (sia sul sistema che sui dati) vengono registrate e riviste periodicamente.
- Il monitoraggio e il rilevamento degli errori di accesso vengono effettuati in modo continuo e identificato i punti deboli sono indirizzati al più presto.

10 VALUTAZIONE DELL'IMPATTO SULLA PROTEZIONE DEI DATI

132. Ai sensi dell'articolo 35, paragrafo 1, i controllori del GDPR sono tenuti a esercitare un impatto sulla protezione dei dati valutazioni (DPIA) quando un tipo di trattamento dei dati può comportare un rischio elevato per i diritti e

libertà delle persone fisiche. L'articolo 35, paragrafo 3, lettera c), del GDPR stabilisce che i controllori sono tenuti a trasportare valutazioni d'impatto sulla protezione dei dati se il trattamento costituisce un monitoraggio sistematico di a area accessibile al pubblico su larga scala. Inoltre, ai sensi dell'articolo 35, paragrafo 3, lettera b), del regolamento generale sulla protezione dei dati a la valutazione dell'impatto della protezione è richiesta anche quando il controllore intende elaborare speciali categorie di dati su larga scala.

133. Le Linee guida sulla valutazione dell'impatto sulla protezione dei dati [27] forniscono ulteriori consigli e informazioni più dettagliate esempi rilevanti per la videosorveglianza (ad esempio, riguardanti "l'uso di un sistema di telecamere per il monitoraggio comportamento di guida in autostrada "). L'articolo 35, paragrafo 4, del regolamento generale sulla protezione dei dati richiede che ciascuna autorità di vigilanza pubblichi un elenco del tipo di operazioni di trattamento soggette alla DPIA obbligatoria all'interno del loro paese. Questi elenchi si trovano di solito sui siti Web delle autorità. Dati gli scopi tipici del video sorveglianza (protezione delle persone e dei beni, individuazione, prevenzione e controllo dei reati,

raccolta di prove e identificazione biometrica di sospetti), è ragionevole supporre che molti
i casi di videosorveglianza richiederanno un DPIA. Pertanto, i responsabili del trattamento dei dati dovrebbero consultare attentamente
questi documenti al fine di determinare se tale valutazione è necessaria e condurla se
necessario. Il risultato del DPIA eseguito dovrebbe determinare la scelta del controller
implementato misure di protezione dei dati.

134. È anche importante notare che se i risultati della DPIA indicano che l'elaborazione comporterebbe un aumento
rischi nonostante le misure di sicurezza pianificate dal responsabile del trattamento, sarà necessario consultare il
autorità di controllo competente prima del trattamento. I dettagli sulle consultazioni precedenti sono disponibili in
Articolo 36.

Per il comitato europeo per la protezione dei dati

La sedia

(Andrea Jelinek)

27 Linee guida per la valutazione dell'impatto sulla protezione dei dati (DPIA) e per determinare se
il trattamento è "suscettibile di comportare un rischio elevato" ai fini del regolamento 2016/679, wp248rev.01,
http://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=611236