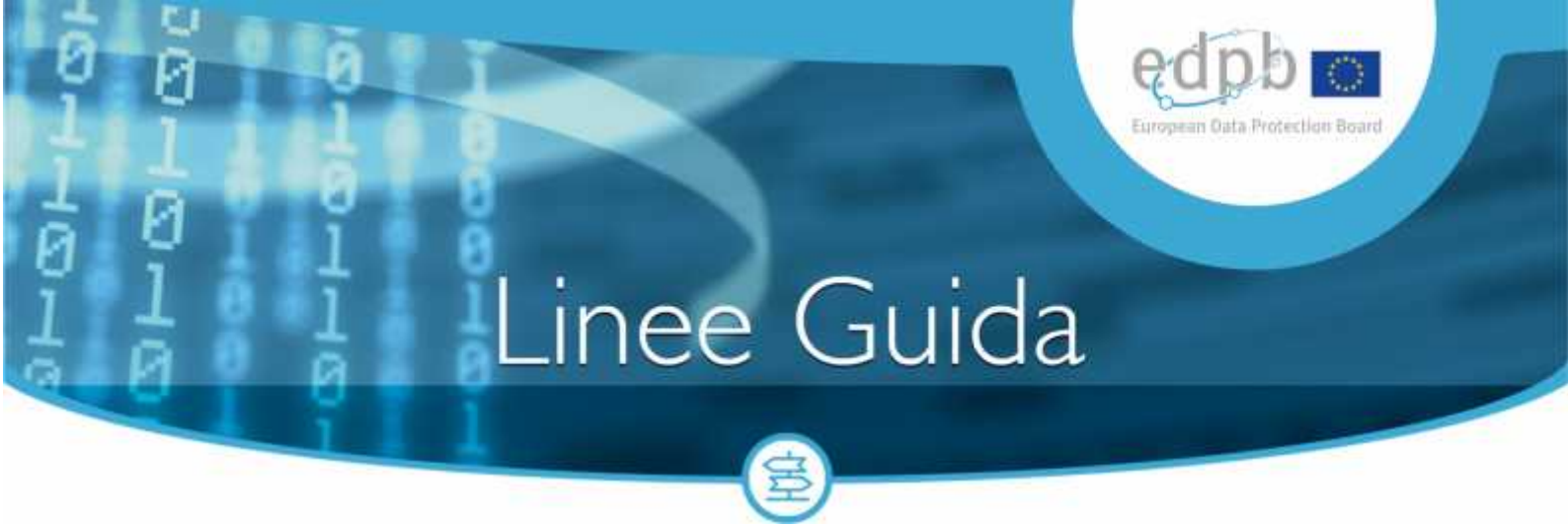


Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video

Versione 2.0

Adottate il 29 gennaio 2020

Cronologia 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 consultazione pubblica

Indice

Il comitato europeo per la protezione dei dati

Considerando l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione 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 («RGPD»),

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

visti l'articolo 12 e l'articolo 22 del regolamento interno,

HA ADOTTATO LE SEGUENTI LINEE GUIDA

1 INTRODUZIONE

1. L'uso intensivo di dispositivi video influisce sul comportamento dei cittadini. Un ricorso significativo a tali strumenti in numerosi ambiti della vita delle persone eserciterà su queste ultime un'ulteriore pressione per impedire il rilevamento di quelle che potrebbero essere percepite come anomalie. Di fatto, queste tecnologie possono limitare le possibilità di muoversi e di utilizzare servizi in maniera anonima nonché, in linea generale, la possibilità di passare inosservati. Le conseguenze per la protezione dei dati sono enormi.

2. Mentre le persone potrebbero essere a proprio agio con la videosorveglianza installata, ad esempio, per una determinata finalità di sicurezza, occorre assicurare che non ne venga fatto un uso improprio per scopi totalmente diversi e inaspettati per l'interessato (ad esempio, per scopi di marketing, controllo delle prestazioni dei dipendenti, ecc.). Inoltre, attualmente si utilizzano molti strumenti per sfruttare le immagini acquisite e trasformare le telecamere tradizionali in telecamere intelligenti. La quantità di dati generati da video, unitamente a questi strumenti e tecniche, aumenta i rischi di un uso secondario (correlato o meno allo scopo al quale viene inizialmente destinato il sistema) o persino improprio. Nel gestire la videosorveglianza sarebbe opportuno considerare sempre attentamente i principi generali del RGPD (articolo 5).

3. I sistemi di videosorveglianza incidono in svariati modi sulle interazioni messe in atto dai professionisti del settore privato e pubblico in luoghi pubblici o privati allo scopo di migliorare la sicurezza, analizzare le risposte del pubblico, fornire pubblicità personalizzata, ecc. La videosorveglianza è diventata un sistema ad alte prestazioni grazie alla crescente applicazione di analisi video intelligenti. Queste tecniche possono essere più intrusive (tecnologie biometriche complesse) o meno intrusive (semplici algoritmi di conteggio). Restare anonimi e preservare la propria privacy è, in linea generale, sempre più difficile. Le questioni relative alla protezione dei dati sollevate nelle diverse situazioni possono essere diverse, così come l'analisi giuridica riferita all'utilizzo dell'una o dell'altra di queste tecnologie.

([1]) Nel presente parere con il termine «Stati membri» si intendono gli «Stati membri del SEE».

4. Oltre alle questioni di privacy, sussistono anche i rischi legati a possibili malfunzionamenti di questi dispositivi e alle distorsioni che possono indurre. I ricercatori riferiscono che il software utilizzato per l'identificazione, il riconoscimento o l'analisi facciale funziona in modo diverso in base all'età, al genere e all'etnia della persona che sta identificando. Le prestazioni degli algoritmi sembrano variare in rapporto ai dati demografici, per cui una distorsione nel riconoscimento facciale minaccia di rafforzare il pregiudizio sociale. Per questo motivo, i titolari del trattamento devono anche assicurare che il trattamento dei dati biometrici derivanti dalla videosorveglianza sia soggetto a una valutazione periodica della sua pertinenza e dell'adeguatezza delle garanzie fornite.

5. La videosorveglianza non è di per sé indispensabile se esistono altri mezzi per raggiungere lo scopo che ci si prefigge. Altrimenti si rischia di modificare le norme culturali con la conseguenza di ammettere come regola l'assenza di privacy .

6. Le presenti linee guida mirano a fornire indicazioni sull'applicazione del RGPD in relazione al trattamento di dati personali attraverso dispositivi video. Gli esempi non sono esaustivi e il ragionamento generale può essere applicato a tutte le potenziali aree di utilizzo.

2 AMBITO DI APPLICAZIONE ([2])

2.1 Dati personali

7. La sorveglianza sistematica e automatizzata di uno spazio specifico con mezzi ottici o audiovisivi, per lo più a scopo di protezione della proprietà, o per proteggere la vita e la salute delle persone, è divenuta un fenomeno significativo dei nostri giorni. Questa attività comporta la raccolta e la conservazione di informazioni grafiche 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 tali persone può essere stabilita sulla base delle informazioni così raccolte. Questo tipo di sorveglianza consente inoltre un ulteriore trattamento dei dati personali per quanto riguarda la presenza e il comportamento delle persone nello spazio considerato. Il rischio potenziale di un uso improprio di tali dati aumenta in rapporto alla dimensione dello spazio monitorato e al numero di persone che lo frequentano. Ciò si riflette nel RGPD all'articolo 35, paragrafo 3, lettera c), che impone l'esecuzione di una valutazione d'impatto sulla protezione dei dati in caso di sorveglianza sistematica su vasta scala di un'area accessibile al pubblico, e all'articolo 37, paragrafo 1, lettera b), che impone ai responsabili del trattamento di designare un responsabile della protezione dei dati se la tipologia di trattamento, per sua natura, richiede il monitoraggio regolare e sistematico degli interessati.

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

> Esempio Il RGPD non è applicabile alle fotocamere false (vale a dire qualsiasi fotocamera che non funziona come una fotocamera e quindi non elabora alcun dato personale). *Tuttavia, in alcuni Stati membri potrebbero essere applicabili altre normative.*
>
> Esempio Le registrazioni ad alta quota rientrano nell'ambito di applicazione del RGPD solo se, in queste circostanze, i dati trattati possono essere correlati a una determinata persona.
>
> Esempio Una videocamera è integrata in un'automobile per fornire assistenza al parcheggio. Se la videocamera è costruita o regolata in modo tale da non raccogliere alcuna informazione relativa a una persona fisica (ad esempio targhe o informazioni che potrebbero identificare i passanti), il RGPD non è applicabile.

9.

2.2 Applicazione della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giudiziarie (direttiva LED)

10. Il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, rientra nella direttiva (UE) 2016/680.

([2]) Il comitato europeo per la protezione dei dati osserva che, laddove il RGPD lo consenta, potrebbero applicarsi requisiti specifici nella legislazione nazionale.

2.3 Deroga relativa alle attività a carattere domestico

11. Ai sensi dell'articolo 2, paragrafo 2, lettera c), il trattamento di dati personali da parte di una persona fisica nel corso di un'attività a carattere esclusivamente personale o domestico, che può anche includere attività online, esula dall'ambito di applicazione del RGPD ([3]).

12. Questa disposizione – la cosiddetta deroga relativa alle attività a carattere domestico – nel contesto della videosorveglianza deve essere interpretata in modo restrittivo. Di conseguenza, come ritenuto dalla Corte di giustizia dell'Unione europea, la cosiddetta «deroga relativa alle attività a carattere domestico» deve *«[…] interpretarsi nel senso che comprende unicamente le attività che rientrano nell'ambito della vita privata o familiare dei singoli, il che manifestamente non avviene nel caso del trattamento di dati personali consistente nella loro pubblicazione su Internet in modo da rendere tali dati accessibili ad un numero indefinito di persone»* ([4]). Inoltre, un sistema di videosorveglianza, nella misura in cui comporta la registrazione e la conservazione costanti di dati personali e si estende *«anche se solo parzialmente, allo spazio pubblico, e pertanto è dirett[o] verso l'esterno della sfera privata della persona che procede al trattamento dei dati con tale modalità, […] non può essere considerat[o] un'attività esclusivamente "personale o domestica" ai sensi dell'articolo 3, paragrafo 2, secondo trattino, della direttiva 95/46»* ([5]).

13. I dispositivi video azionati all'interno dei locali di un privato possono rientrare nella deroga relativa alle attività a carattere domestico. Ciò dipenderà da diversi fattori, che dovranno essere presi in considerazione nella loro totalità per giungere a una conclusione. Oltre agli elementi summenzionati individuati dalle sentenze della Corte di giustizia dell'Unione europea, chi utilizza la videosorveglianza presso il proprio domicilio deve verificare se ha un qualche tipo di rapporto personale con l'interessato, se la portata o la frequenza della sorveglianza siano indicative di una qualche forma di attività professionale da parte sua e il potenziale impatto negativo della sorveglianza sugli interessati. La presenza di uno qualsiasi degli elementi summenzionati non implica necessariamente che il trattamento non rientri nell'ambito di applicazione della deroga relativa alle attività a carattere domestico; per stabilirlo è infatti necessaria una valutazione complessiva.

([3]) Cfr. anche il considerando 18.

([4]) Corte di giustizia dell'Unione europea, sentenza nella causa C-101/01*, Bodil Lindqvist,* 6 novembre 2003, punto 47.

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

Esempio Per documentare le sue vacanze, un turista registra video sia con il suo cellulare sia con una videocamera. Mostra il filmato ad amici e familiari, ma non lo rende accessibile a un numero indefinito di persone. Questo caso rientrerebbe nella deroga relativa alle attività a carattere domestico.

Esempio Una ciclista in mountain bike vuole registrare il suo percorso in discesa con una telecamera sportiva. Attraversa una zona isolata e prevede di utilizzare le registrazioni solo per intrattenimento personale e nel suo domicilio. Questo caso rientrerebbe nella deroga relativa alle attività a carattere domestico anche se vi fosse in una certa misura un trattamento di dati personali.

Esempio: Qualcuno sorveglia e registra il proprio giardino. La proprietà è recintata e soltanto il titolare del trattamento e la sua famiglia entrano regolarmente in giardino. Questo caso rientrerebbe nella deroga relativa alle attività a carattere domestico, a condizione che la videosorveglianza non si estenda, neppure parzialmente, a uno spazio pubblico o a una proprietà confinanti.

14.

3 LICEITÀ DEL TRATTAMENTO

15. Prima di procedere, si devono specificare dettagliatamente le finalità del trattamento (articolo 5, paragrafo 1, lettera b)). La videosorveglianza può servire a molti scopi, ad esempio a supporto della protezione della proprietà e di altri beni, della protezione della vita e dell'integrità fisica delle persone o a raccogliere elementi di prova in vista di procedimenti giudiziari civili ([6]). Queste finalità del monitoraggio devono essere documentate per iscritto (articolo 5, paragrafo 2) e devono essere specificate per ogni telecamera di sorveglianza in uso. Le telecamere utilizzate per lo stesso scopo da un unico titolare del trattamento possono essere oggetto di una documentazione unitaria. Inoltre, gli interessati devono essere informati delle finalità del trattamento ai sensi dell'articolo 13 (*si veda la sezione 7, Obblighi di trasparenza e di informazione*). La semplice menzione di uno scopo di «sicurezza» o «per la vostra sicurezza» con riguardo alla videosorveglianza non è sufficientemente specifica (articolo 5, paragrafo 1, lettera b)). Ciò contrasta inoltre con il principio secondo il quale i dati personali vengono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato [cfr. articolo 5, paragrafo 1, lettera a)].

16. In linea di principio, ogni fondamento di diritto ai sensi dell'articolo 6, paragrafo 1, può fornire una base giuridica per il trattamento dei dati di videosorveglianza. Ad esempio, l'articolo 6, paragrafo 1, lettera c), si applica quando la normativa nazionale prevede l'obbligo di mettere in atto in sistema di videosorveglianza ([7]). Tuttavia, nella pratica, le disposizioni più suscettibili di essere utilizzate sono

- Articolo 6, paragrafo 1, lettera f) (legittimo interesse)
- Articolo 6, paragrafo 1, lettera e) (necessità al fine di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri).

In casi piuttosto eccezionali il titolare del trattamento potrebbe invocare l'articolo 6, paragrafo 1, lettera a) (consenso) come base giuridica .

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

17. L'analisi giuridica della disposizione contenuta all'articolo 6, paragrafo 1, lettera f), dovrebbe basarsi sui criteri indicati di seguito, conformemente al considerando 47.

3.1.1 Esistenza di legittimi interessi

18. La videosorveglianza è lecita se è necessaria per conseguire la finalità di un legittimo interesse perseguito da un titolare del trattamento o da un terzo, a meno che su tali interessi prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato (articolo 6, paragrafo 1, lettera f)). I legittimi interessi perseguiti da un titolare del trattamento o da terzi possono avere natura giuridica ([8]), economica o immateriale ([9]). Tuttavia, il titolare del trattamento dovrebbe considerare che se l'interessato si oppone alla sorveglianza a norma dell'articolo 21, si può procedere alla videosorveglianza di tale interessato soltanto se il legittimo interesse in questione ha natura *cogente*

([6]) Le norme sulla raccolta di prove nei procedimenti civili variano da uno Stato membro all'altro.

([7]) Le presenti linee guida non analizzano né approfondiscono la normativa nazionale che potrebbe differire da uno Stato membro all'altro.

([8]) Corte di giustizia dell'Unione europea, sentenza nella causa C-13/16, *Rīgas satiksme*, 4 maggio 2017

([9]) Cfr. WP217, gruppo di lavoro "Articolo 29".

e prevale sugli interessi, i diritti e le libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

19. In presenza di una situazione di reale rischio, la tutela della proprietà da furti o atti vandalici può costituire un legittimo interesse con riguardo alla videosorveglianza.

20. Il legittimo interesse deve essere esistente e attuale (ossia non deve essere fittizio o ipotetico) ([10]). Prima di avviare la sorveglianza è necessario che sussista una situazione di reale difficoltà, come ad esempio danni o incidenti gravi verificatisi in passato. Alla luce del principio di responsabilizzazione, i titolari del trattamento farebbero bene a documentare gli eventi problematici in questione (data, modalità, perdita finanziaria) e le relative accuse penali. Tali casi documentati possono costituire un solido elemento di prova per l'esistenza di un legittimo interesse. L'esistenza di un legittimo interesse e la necessità del monitoraggio dovrebbero essere oggetto di riesame periodico (ad esempio, una volta all'anno, a seconda delle circostanze).

> Esempio Un negoziante vuole aprire un nuovo esercizio commerciale e installare un sistema di videosorveglianza per prevenire atti vandalici. Può dimostrare, presentando delle statistiche, che nel quartiere è alta la probabilità di eventi vandalici . E' utile anche l'esperienza degli esercizi commerciali posti in prossimità. Non è necessario che il titolare del trattamento in questione abbia subito un danno. Nella misura in cui dai danni subiti nel quartiere emerga una situazione di pericolo o comunque analoga, può esservi un'indicazione dell'esistenza di un legittimo interesse. Tuttavia, non è sufficiente presentare statistiche nazionali o generali sulla criminalità senza analizzare l'area in questione o i pericoli per lo specifico esercizio commerciale.

21.

22. Le situazioni di pericolo imminente possono configurare un legittimo interesse, per esempio nel caso di banche o negozi che vendono beni preziosi (ad esempio, gioiellerie) o di luoghi che sono notoriamente teatro di reati contro il patrimonio (ad esempio, stazioni di servizio).

23. Il RGPD stabilisce inoltre chiaramente che le autorità pubbliche non possono invocare il legittimo interesse per i trattamenti svolti nell'esecuzione dei loro compiti. Cfr. articolo 6, paragrafo 1, seconda frase.

3.1.2 Necessità del trattamento

24. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario rispetto 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 titolare del trattamento deve sempre valutare criticamente se questa misura sia in primo luogo idonea a raggiungere l'obiettivo desiderato e, in secondo luogo, adeguata e necessaria per i suoi scopi. Si dovrebbe optare per misure di videosorveglianza unicamente se la finalità del trattamento non può ragionevolmente essere raggiunta con altri mezzi meno intrusivi per i diritti e le libertà fondamentali dell'interessato.

25. In una situazione in cui un titolare del trattamento intenda prevenire reati legati al patrimonio, invece di installare un sistema di videosorveglianza potrebbe adottare misure di sicurezza alternative, come la recinzione della proprietà, il pattugliamento regolare di personale di sicurezza, l'impiego di custodi, una migliore illuminazione, l'installazione di serrature di sicurezza, finestre e porte a prova di manomissione o l'applicazione di rivestimento anti-graffiti o lamine alle pareti. Tali misure possono

([10]) Cfr. WP217, Gruppo di lavoro "Articolo 29", pag. 24 e segg. Cfr. anche la causa C-708/18 della Corte di giustizia dell'Unione europea, punto 44.

essere efficaci quanto i sistemi di videosorveglianza contro furti e vandalismi. Il titolare del trattamento deve valutare caso per caso se tali misure possano essere una soluzione ragionevole.

26. Prima di utilizzare un sistema di telecamere, il titolare del trattamento è tenuto a valutare dove e quando siano assolutamente necessarie misure di videosorveglianza. Di solito un sistema di sorveglianza funzionante sia di notte sia al di fuori del normale orario di lavoro soddisfa le esigenze del titolare del trattamento di prevenire pericoli per il suo patrimonio.

27. In generale, la necessità di utilizzare la videosorveglianza per proteggere la proprietà di un titolare si arresta ai confini della proprietà stessa.[11] Tuttavia, vi sono casi in cui la sorveglianza della proprietà non è sufficiente per una protezione efficace. In alcuni singoli casi potrebbe essere necessario estendere la videosorveglianza alle immediate vicinanze dell'area di proprietà. In tale contesto, il titolare del trattamento dovrebbe prendere in considerazione l'impiego di mezzi fisici e tecnici, ad esempio bloccando o oscurando le zone non pertinenti.

> Esempio Una libreria vuole proteggere la propria sede contro atti di vandalismo. In linea generale, le telecamere dovrebbero riprendere soltanto i locali in senso stretto; non è infatti necessario sorvegliare i locali adiacenti o le zone pubbliche circostanti la sede della libreria per tale scopo.

28.

29. Occorre interrogarsi sulla necessità del trattamento anche per quanto riguarda le modalità di conservazione di elementi di prova . In alcuni casi potrebbe essere necessario utilizzare soluzioni tipo scatola nera, nelle quali il filmato viene automaticamente cancellato dopo un determinato periodo di conservazione e vi si accede solo in caso di eventi problematici. In altre situazioni potrebbe non essere affatto necessario registrare il materiale video, essendo magari più opportuno ricorrere al monitoraggio in tempo reale. La scelta tra le due soluzioni dovrebbe anche basarsi sullo scopo perseguito. Se, ad esempio, la videosorveglianza è finalizzata alla raccolta di prove, solitamente i metodi in tempo reale non sono adatti. Talvolta il monitoraggio in tempo reale può risultare anche più intrusivo rispetto alla conservazione e alla cancellazione automatica delle registrazioni dopo un lasso di tempo limitato (ad esempio, se un operatore visualizza costantemente le immagini su monitor, questo metodo potrebbe essere più intrusivo rispetto alla conservazione diretta del materiale in una scatola nera in assenza di monitoraggio). In questo contesto occorre avere riguardo al principio della minimizzazione dei dati (articolo 5, paragrafo 1, lettera c)). Occorre inoltre tenere presente la possibilità per il titolare del trattamento di avvalersi di personale di sicurezza in grado di reagire e intervenire immediatamente anziché ricorrere alla videosorveglianza.

3.1.3 Bilanciamento degli interessi

30. Supponendo che la videosorveglianza sia necessaria per proteggere i legittimi interessi di un titolare del trattamento, un sistema di videosorveglianza può essere messo in funzione unicamente se sui legittimi interessi del titolare del trattamento o su quelli di terzi (ad esempio, la protezione della proprietà o dell'integrità fisica) non prevalgono gli interessi o i diritti e le libertà fondamentali dell'interessato. Il titolare del trattamento deve valutare 1) in che misura il monitoraggio incida sugli interessi, sui diritti fondamentali e sulle libertà degli individui, e 2) se ciò comporti violazioni o conseguenze negative rispetto ai diritti dell'interessato. Di fatto, il bilanciamento degli interessi è

([11]) In alcuni Stati membri ciò potrebbe anche essere soggetto alla normativa nazionale.

d'obbligo. I diritti e le libertà fondamentali, da un lato, e i legittimi interessi del titolare del trattamento, dall'altro, vanno valutati e bilanciati con attenzione.

> Esempio Una società che gestisce un parcheggio privato ha registrato problemi ricorrenti di furti nelle auto parcheggiate. Il parcheggio è uno spazio aperto e facilmente accessibile da chiunque, ma è chiaramente contrassegnato con cartelli e dissuasori che circondano l'area interessata. La società di parcheggio ha un legittimo interesse (prevenire i furti nelle auto dei clienti) a monitorare l'area durante le ore del giorno in cui si verificano problemi. Gli interessati sono sorvegliati per un arco di tempo limitato, non si trovano nella zona per scopi ricreativi ed è anche nel loro interesse prevenire i furti. In questo caso, sull'interesse degli interessati a non essere sottoposti a monitoraggio prevale il legittimo interesse del titolare del trattamento.
>
> Esempio Un ristorante decide di installare videocamere nei bagni per controllare la pulizia dei servizi igienici. In questo caso i diritti degli interessati prevalgono chiaramente sull'interesse del titolare del trattamento, pertanto le telecamere non possono essere installate.

31.

3.1.3.1 Decidere caso per caso

32. Poiché il bilanciamento degli interessi è obbligatorio 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 casi simili tra loro. Il titolare del trattamento deve valutare i rischi di interferenza nei diritti dell'interessato; in questo caso il criterio decisivo è l'intensità dell'intervento rispetto ai diritti e allele libertà dell'individuo.

33. L'intensità può essere definita, tra l'altro, dal tipo di informazioni raccolte (contenuto delle informazioni), dalla portata (densità delle informazioni, estensione territoriale e geografica), dal numero di interessati coinvolti – come numero specifico o come percentuale della popolazione interessata – dalla situazione specifica, dagli interessi effettivi del gruppo di interessati, dalla disponibilità di strumenti mezzi alternativi nonché dalla natura e dalla portata della valutazione dei dati.

34. Importanti fattori di bilanciamento possono essere le dimensioni della zona e il numero di interessati sotto sorveglianza. L'uso della videosorveglianza in una zona isolata (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 è installata una telecamera da cruscotto (dash cam) – ad esempio, allo scopo di raccogliere prove in caso di incidente – è importante assicurarsi che la telecamera non registri costantemente il traffico, così come le persone che si trovano vicino a una strada. In caso contrario, l'interesse ad avere le videoregistrazioni come elemento di prova nel caso ipotetico di un incidente stradale non può giustificare questa grave interferenza nei diritti degli interessati ([11]).

35.

3.1.3.2 Ragionevoli aspettative degli interessati

36. Secondo il considerando 47, l'esistenza di un legittimo interesse richiede un'attenta valutazione. A questo proposito, occorre includere le ragionevoli aspettative dell'interessato al momento e nel contesto del trattamento dei suoi dati personali. Per quanto riguarda la sorveglianza sistematica, il rapporto tra l'interessato e il titolare del trattamento può variare significativamente e può influenzare

le ragionevoli aspettative dell'interessato. L'interpretazione del concetto di aspettativa ragionevole non dovrebbe basarsi soltanto sulle aspettative soggettive in questione. Il criterio decisivo deve essere invece se un soggetto terzo imparziale possa ragionevolmente aspettarsi e concludere di essere oggetto di sorveglianza nella situazione specifica.

37. Ad esempio, nella maggior parte dei casi un dipendente sul luogo di lavoro non si aspetta di essere monitorato dal proprio datore di lavoro ([12]). Inoltre, non ci si aspetta sorveglianza nel proprio giardino, in locali abitati o in ambulatori e sale di terapia. Analogamente, non è ragionevole aspettarsi sorveglianza nei servizi sanitari o nelle saune; la sorveglianza in questo tipo di zone costituisce una grave interferenza nei diritti dell'interessato. Le ragionevoli aspettative degli interessati sono quindi che non si attui alcuna videosorveglianza in tali zone. D'altro canto, il cliente di una banca potrebbe aspettarsi di essere sorvegliato all'interno della banca o presso un bancomat.

38. Gli interessati possono anche aspettarsi di non essere sorvegliati all'interno di aree accessibili al pubblico – soprattutto se tali aree sono solitamente utilizzate per la convalescenza, la rigenerazione e per attività ricreative – nonché nei luoghi in cui le persone trascorrono del tempo e/o interagiscono, come ad esempio zone 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 spesso prevarranno sui legittimi interessi del titolare del trattamento.

> Esempio Nei servizi igienici gli interessati si aspettano di non essere sorvegliati. La videosorveglianza, ad esempio, per prevenire incidenti non è uno strumento proporzionato.

39.

40. La presenza di segnaletica che informa l'interessato in merito alla videosorveglianza è del tutto irrilevante al fine di determinare ciò che un interessato può oggettivamente aspettarsi. Ciò significa, ad esempio, che il proprietario di un esercizio commerciale non può fare affidamento sull'esistenza oggettiva di una ragionevole aspettativa da parte dei clienti riguardo al monitoraggio solo perché un cartello all'ingresso li informa della presenza di un sistema di sorveglianza.

3.2 Necessità allo scopo di eseguire un compito nell'interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (articolo 6, paragrafo 1, lettera e)).

41. I dati personali potrebbero essere trattati mediante la videosorveglianza a norma dell'articolo 6, paragrafo 1, lettera e), se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri ([13]). Può darsi che l'esercizio di pubblici poteri non consenta tale trattamento, ma altri fondamenti di liceità, per esempio obiettivi di «salute e sicurezza» per la protezione di visitatori e dipendenti, possono fornire un margine limitato per il trattamento, in ogni caso tenendo conto degli obblighi previsti dal RGPD e dei diritti degli interessati.

([12]) Cfr. anche: Gruppo di lavoro "Articolo 29", parere 2/2017 sul trattamento dei dati sul luogo di lavoro, WP 249, adottato l'8 giugno 2017.

([13]) La base su cui si fonda il trattamento dei dati in questione deve essere stabilita dal diritto dell'Unione o dal diritto degli Stati membri ed è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (articolo 6, paragrafo 3).

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

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

43. Il consenso deve essere prestato liberamente, deve essere specifico, informato e inequivocabile, come descritto nelle linee guida sul consenso ([14]).

44. Per quanto riguarda la sorveglianza sistematica, il consenso dell'interessato può fungere da base giuridica ai sensi dell'articolo 7 (cfr. il considerando 43) solo in casi eccezionali. È nella natura della sorveglianza il fatto che questa tecnologia consenta di controllare contemporaneamente un numero non noto di persone. Il titolare del trattamento difficilmente sarà in grado di dimostrare che l'interessato ha prestato il consenso prima del trattamento dei suoi dati personali (articolo 7, paragrafo 1). Supponendo che l'interessato revochi il proprio consenso, sarà difficile per il titolare dimostrare che i dati personali non sono più oggetto di trattamento (articolo 7, paragrafo 3).

> Esempio Gli atleti possono chiedere di essere monitorati durante gli esercizi individuali al fine di analizzare tecniche e prestazioni. D'altra parte, quando una società sportiva prende l'iniziativa di monitorare un'intera squadra per la stessa finalità, il consenso spesso non sarà valido, in quanto i singoli atleti possono sentirsi costretti a prestare il proprio consenso per evitare che un loro eventuale rifiuto si ripercuota negativamente sui compagni di squadra.

45.

46. Se il titolare del trattamento desidera invocare il consenso, è suo dovere assicurarsi che ogni interessato che entra nella zona sottoposta a videosorveglianza abbia prestato il proprio consenso. Tale consenso deve soddisfare le condizioni di cui all'articolo 7. L'ingresso in una zona sorvegliata contrassegnata (ad esempio, le persone sono invitate a passare attraverso uno specifico corridoio o cancello per accedere a una zona sorvegliata), non configura una dichiarazione o una chiara azione affermativa come necessarie per la validità del consenso, a meno che siano soddisfatti i criteri di cui agli articoli 4 e 7 descritti 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 invocare il consenso nel trattare i dati personali, in quanto è improbabile che quest'ultimo venga fornito liberamente. In tale contesto si dovrebbe tener conto delle linee guida sul consenso.

48. La legge degli Stati membri o i contratti collettivi, compresi i «contratti di lavoro», possono prevedere norme specifiche sul trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro (cfr. l'articolo 88).

([14]) Gruppo di lavoro "Articolo 29": «Linee guida sul consenso ai sensi del regolamento (UE) 2016/679» (WP 259 rev. 01) – approvate dal comitato europeo per la protezione dei dati.

([15]) Gruppo di lavoro "Articolo 29", «Linee guida sul consenso ai sensi del regolamento (UE) 2016/679» (WP 259) – approvate dal comitato europeo per la protezione dei dati – di cui si dovrebbe tener conto.

4 COMUNICAZIONE DI FILMATI A TERZI

49. In linea di principio, le norme generali del RGPD si applicano alla comunicazione di videoregistrazioni a soggetti terzi.

4.1 Comunicazione di filmati a soggetti terzi in generale

50. La comunicazione è definita all'articolo 4, paragrafo 2, come trasmissione (comunicazione individuale), diffusione (pubblicazione online) o qualsiasi altra forma di messa a disposizione. I soggetti terzi sono definiti all'articolo 4, paragrafo 10. In caso di comunicazione a paesi terzi o organizzazioni internazionali, si applicano anche le disposizioni speciali dall'articolo 44 e seguenti.

51. Qualsiasi comunicazione di dati personali costituisce uno specifico trattamento per il quale il titolare deve avere una base giuridica fra quelle di cui all'articolo 6.

> Esempio Il titolare del trattamento che desidera caricare una registrazione su Internet deve fare riferimento a 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 a terzi per scopi diversi da quelli per i quali i dati sono stati raccolti è possibile a norma dell'articolo 6, paragrafo 4.

> Esempio La barriera di un parcheggio è videosorvegliata allo scopo di risolvere le cause per danni. Quando si verifica un danno, la registrazione viene ceduta a un avvocato per la trattazione di una causa. In questo caso lo scopo della registrazione coincide con quello della trasmissione.
>
> Esempio La barriera di un parcheggio è videosorvegliata allo scopo di risolvere le cause per danni. La registrazione viene pubblicata online per puro divertimento. In questo caso lo scopo è diverso e non è compatibile con lo scopo iniziale. Sarebbe inoltre problematico individuare una base giuridica per tale trattamento (pubblicazione).

54.

55. Il terzo destinatario dovrà effettuare una propria analisi giuridica, in particolare individuando la base giuridica del suo trattamento (per esempio, la ricezione dei materiali filmati) ai sensi dell'articolo 6 .

4.2 Comunicazione di filmati alle autorità di contrasto

56. Anche la comunicazione di videoregistrazioni alle autorità di contrasto è un processo indipendente, per il quale il titolare del trattamento deve individuare una separata giustificazione.

57. Secondo l'articolo 6, paragrafo 1, lettera c), il trattamento è lecito se è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento. Sebbene le attività di polizia siano disciplinate in via esclusiva dalle norme vigenti nei singoli Stati membri, è molto probabile che esistano norme generali che disciplinano il trasferimento delle prove alle autorità di contrasto in ogni Stato membro. Il trattamento eseguito dal titolare che consegna i dati è disciplinato dal RGPD. Se la normativa nazionale impone al titolare del trattamento di cooperare con le autorità di contrasto (per esempio nelle indagini), la base giuridica per la trasmissione dei dati è un obbligo legale di cui all'articolo 6, paragrafo 1, lettera c).

58. Spesso, quindi, il rispetto dei requisiti di limitazione della finalità di cui all'articolo 6, paragrafo 4, non risulta problematico, in quanto la comunicazione è disciplinata esplicitamente dal diritto degli Stati membri. Non è quindi necessario prendere in considerazione i requisiti specifici riferiti all'eventuale cambiamento di finalità ai sensi delle lettere a)-e) dell'Articolo 6, paragrafo 4.

59. Esempio Il proprietario di un esercizio commerciale registra i filmati dell'impianto di videosorveglianza posto all'ingresso dello stesso. Un filmato mostra una persona che ruba il portafoglio di un'altra persona. La polizia chiede al titolare del trattamento di consegnare il materiale per assisterla nelle indagini. In questo caso, il proprietario dell'esercizio commerciale utilizzerebbe la base giuridica di cui all'articolo 6, paragrafo 1, lettera c) (obbligo legale), in combinato disposto con la normativa nazionale applicabile per il trattamento consistente nella comunicazione dei materiali.

60. Esempio Una telecamera viene installata in un esercizio commerciale per motivi di sicurezza. Il proprietario crede di aver registrato qualcosa di sospetto e decide di inviare il materiale alla polizia (senza alcuna indicazione che vi sia un'indagine in corso). In questo caso il proprietario dell'esercizio commerciale deve valutare se sono soddisfatte le condizioni previste, nella maggior parte dei casi, dall'articolo 6, paragrafo 1, lettera f) – come per esempio qualora abbia un ragionevole sospetto che sia stato commesso un reato.

61. Il trattamento dei dati personali da parte delle autorità di contrasto non è disciplinato dal RGPD (si veda l'articolo 2, paragrafo 2, lettera d)), bensì dalla direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giudiziarie.

5 TRATTAMENTI RIGUARDANTI CATEGORIE PARTICOLARI DI DATI

62. Solitamente, i sistemi di videosorveglianza raccolgono enormi quantità di dati personali che possono rivelare dati di natura altamente personale e persino categorie particolari di dati. Infatti, dati apparentemente non significativi, all'origine raccolti tramite video, possono essere utilizzati per ricavare altre informazioni e raggiungere uno scopo diverso da quello iniziale (ad esempio per mappare le abitudini di un individuo). Tuttavia, la videosorveglianza non sempre è considerata un trattamento di categorie particolari di dati personali.

> Esempio Le riprese video che mostrano un interessato che indossa occhiali o utilizza una sedia a rotelle non sono di per sé considerate categorie particolari di dati personali.

63.

64. Tuttavia, se le riprese video sono trattate per ricavare categorie particolari di dati, si applica l'articolo 9.

> Esempio Si potrebbero, ad esempio, dedurre le opinioni politiche da immagini che mostrano interessati identificabili mentre partecipano a un evento, a uno sciopero, ecc. Questo caso rientrerebbe nell'ambito di applicazione dell'articolo 9.
>
> Esempio Un ospedale che installa una videocamera per monitorare le condizioni di salute di un paziente effettua un trattamento di categorie particolari di dati personali (articolo 9).

65.

66. In via generale e in linea di principio, ogniqualvolta si installa un sistema di videosorveglianza si dovrebbe prestare particolare attenzione al principio della minimizzazione dei dati. Pertanto, anche nei casi in cui l'articolo 9, paragrafo 1, non si applica, il titolare del trattamento dovrebbe sempre cercare di ridurre al minimo il rischio di acquisire filmati che rivelino altri dati sensibili (al di là dell'articolo 9), indipendentemente dalla finalità.

> Esempio Un'attività di videosorveglianza che acquisisce le immagini di una chiesa non rientra di per sé nel campo di applicazione dell'articolo 9. Tuttavia, il titolare del trattamento deve effettuare una valutazione particolarmente attenta ai sensi dell'articolo 6, paragrafo 1, lettera f), con riguardo agli interessi della persona interessata, tenendo conto della natura dei dati nonché del rischio di acquisire altri dati sensibili (ulteriori rispetto a quelli di cui all'articolo 9) .

67.

68. Se un sistema di videosorveglianza è utilizzato per trattare categorie particolari di dati, il titolare del trattamento deve individuare sia un'eccezione che consenta il trattamento di categorie particolari di dati ai sensi dell'articolo 9 (vale a dire un'esenzione dal divieto generale di trattare categorie particolari di dati) sia una base giuridica ai sensi dell'articolo 6.

69. Ad esempio, si potrebbe utilizzare l'articolo 9, paragrafo 2, lettera c) («[…] *il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica* […]») – in teoria e in via del tutto eccezionale – ma il titolare del trattamento dovrebbe giustificarlo come una necessità assoluta per tutelare gli interessi vitali di tale persona e dimostrare che «[…] l'interessato *si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso*». Inoltre, il titolare del trattamento non potrà utilizzare il sistema per nessun altro motivo.

70. È importante rilevare in questa sede che probabilmente non tutte le esenzioni elencate all'articolo 9 sono utilizzabili per giustificare il trattamento di categorie particolari di dati attraverso la videosorveglianza. Più specificamente, i titolari che trattano tali dati nell'ambito della videosorveglianza non possono invocare l'articolo 9, paragrafo 2, lettera e), che consente il trattamento di dati personali resi manifestamente pubblici dall'interessato. Il semplice fatto di entrare nell'area di ripresa della telecamera non implica che l'interessato intenda rendere pubbliche categorie particolari di dati che lo riguardano.

71. Inoltre, il trattamento di categorie particolari di dati richiede una vigilanza rafforzata e continua su taluni obblighi, ad esempio un elevato livello di sicurezza e una valutazione d'impatto sulla protezione dei dati, ove necessario.

> Esempio Un datore di lavoro non deve utilizzare registrazioni di videosorveglianza che mostrano una manifestazione al fine di identificare gli scioperanti.

72.

5.1 Considerazioni generali sul trattamento dei dati biometrici

73. L'uso di dati biometrici, in particolare il riconoscimento facciale, comporta maggiori rischi per i diritti degli interessati. È fondamentale che il ricorso a tali tecnologie avvenga nel dovuto rispetto dei principi di liceità, necessità, proporzionalità e minimizzazione dei dati sanciti nel RGPD. Sebbene l'uso di queste tecnologie possa essere percepito come particolarmente efficace, i titolari del trattamento dovrebbero in primo luogo valutare l'impatto sui diritti e sulle libertà fondamentali e considerare mezzi meno intrusivi per raggiungere il legittimo scopo del rispettivo trattamento.

74. Per poter configurare un trattamento di dati biometrici, secondo la definizione del RGPD, il trattamento di dati grezzi, come ad esempio le caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, deve comprendere una misurazione di tali caratteristiche. Poiché i dati biometrici sono il risultato di dette misurazioni, il RGPD afferma nel suo articolo 4, paragrafo 14, che sono dati «*[…] ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca […]*». Tuttavia, le riprese video di un individuo non possono essere considerate di per sé dati biometrici ai sensi dell'articolo 9, se non sono state sottoposte a un trattamento tecnico specifico per contribuire all'identificazione di tale individuo ([16]).

75. Affinché il trattamento sia considerato un trattamento di categorie particolari di dati personali (articolo 9), è necessario che siano trattati dati biometrici «intesi a identificare in modo univoco una persona fisica».

76. Riassumendo, alla luce dell'articolo 4, paragrafo 14, e dell'articolo 9, si devono prendere in considerazione tre criteri:

- **natura dei dati**: dati relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica;
- **mezzi e modalità del trattamento**: dati «ottenuti da un trattamento tecnico specifico»;

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

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

77. L'uso della videosorveglianza associata alla funzionalità del riconoscimento biometrico da parte di soggetti privati per proprie finalità (ad esempio, marketing, statistiche o persino 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 deroga idonea di cui all'articolo 9.

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

Esempio Un titolare del trattamento gestisce l'accesso al proprio edificio utilizzando un metodo di riconoscimento facciale. L'utilizzo di questa modalità di accesso è possibile solo se gli interessati hanno preventivamente prestato il loro consenso informato ed esplicito (ai sensi dell'articolo 9, paragrafo 2, lettera a)). Tuttavia, al fine di garantire che non vengano acquisiti i dati di coloro che non abbiano precedentemente prestato il consenso, il riconoscimento facciale dovrebbe essere attivato dall'interessato stesso, ad esempio premendo un pulsante. Per assicurare la liceità del trattamento, il titolare deve sempre offrire una modalità alternativa di accesso all'edificio senza trattamento biometrico, ad esempio tramite badge o chiavi.

78.

79. In questi casi, in cui vengono generati modelli biometrici, i titolari del trattamento devono garantire che, una volta ottenuta una corrispondenza o non corrispondenza, tutti i modelli intermedi realizzati in tempo reale (con il consenso esplicito e informato dell'interessato) al fine del raffronto con quelli creati dagli interessati all'atto della registrazione, siano cancellati immediatamente e in modo sicuro. I modelli creati per la registrazione dovrebbero essere conservati esclusivamente per la realizzazione della finalità del trattamento e non dovrebbero essere conservati né archiviati.

80. Tuttavia, quando la finalità del trattamento è, ad esempio, distinguere fra categorie di persone anziché identificare in modo univoco una specifica persona, il trattamento non è disciplinato dall'articolo 9.

Esempio Il proprietario di un esercizio commerciale vorrebbe personalizzare la propria pubblicità in base al genere e all'età dei clienti, acquisendo tali caratteristiche attraverso un sistema di videosorveglianza. Se tale sistema non genera modelli biometrici al fine di identificare in modo univoco le persone, ma semplicemente rileva tali caratteristiche fisiche al fine di classificare le persone, il trattamento non ricade nel campo di applicazione dell'articolo 9 (purché non siano trattate altre categorie particolari di dati).

81.

82. Tuttavia, l'articolo 9 si applica se il titolare del trattamento conserva i dati biometrici (comunemente attraverso modelli creati estraendo le caratteristiche chiave dalla forma grezza dei dati biometrici, ad esempio misurazioni facciali ricavate da un'immagine), al fine di identificare in modo univoco una persona. Se un titolare del trattamento desidera individuare un interessato che rientra nella zona sorvegliata o entra in un'altra zona (ad esempio, per proiettare annunci pubblicitari personalizzati in modo continuo), in questo caso lo scopo sarebbe quello di identificare in modo univoco una persona fisica e quindi l'operazione rientrerebbe fin dall'inizio nel campo di applicazione dell'articolo 9. Ciò potrebbe accadere se il titolare conserva i modelli generati per fornire ulteriore pubblicità personalizzata su diversi cartelloni pubblicitari in vari punti all'interno del negozio. Poiché il sistema utilizza caratteristiche fisiche per individuare soggetti specifici che tornano nell'area di ripresa della telecamera (come i visitatori di un centro commerciale) e li traccia, questa funzione costituirebbe un metodo di identificazione biometrica perché è finalizzata al riconoscimento attraverso l'uso di un trattamento tecnico specifico.

> Esempio Un negoziante ha installato un sistema di riconoscimento facciale all'interno del proprio negozio al fine di personalizzare la pubblicità rivolta ai clienti. Il titolare del trattamento deve ottenere il consenso esplicito e informato di tutti gli interessati prima di utilizzare questo sistema biometrico e trasmettere pubblicità personalizzata. Il sistema sarebbe illegale se acquisisse i dati dei visitatori o dei passanti che non hanno acconsentito alla creazione di un modello biometrico, anche se quest'ultimo venisse eliminato nel più breve tempo possibile. Infatti, questi modelli temporanei costituiscono dati biometrici trattati al fine di identificare in modo univoco una persona che potrebbe non voler ricevere pubblicità mirata.

83.

84. Il comitato europeo per la protezione dei dati osserva che alcuni sistemi biometrici sono installati in ambienti non controllati ([17]), il che significa che il sistema comporta l'acquisizione in tempo reale dei volti di qualsiasi individuo che entra nell'area di ripresa della telecamera, comprese le persone che non hanno acconsentito al dispositivo biometrico, con la successiva creazione di modelli biometrici. Questi modelli vengono confrontati con quelli creati dagli interessati che hanno prestato il previo consenso durante un processo di registrazione (vale a dire gli utenti del dispositivo biometrico) al fine di consentire al titolare del trattamento di riconoscere se la persona utilizzi o meno il dispositivo biometrico. In questo caso, il sistema è spesso progettato per distinguere i soggetti da riconoscere fra quelli inseriti in una banca dati rispetto ai soggetti non registrati. Poiché lo scopo è quello di identificare in modo univoco persone fisiche, è comunque necessaria l'applicazione di una delle deroghe di cui all'articolo 9, paragrafo 2, del RGPD per trattare i dati di chiunque sia ripreso dalla telecamera.

([17]) Significa che il dispositivo biometrico è ubicato in uno spazio aperto al pubblico ed è in grado di funzionare su chiunque passi di lì, al contrario dei sistemi biometrici in ambienti controllati, che possono essere utilizzati soltanto con la partecipazione di una persona consenziente.

Esempio Un hotel utilizza la videosorveglianza per avvisare automaticamente il direttore dell'arrivo di un VIP nel momento in cui il volto dell'ospite viene riconosciuto. I VIP in questione hanno prestato preventivamente il consenso esplicito all'uso del riconoscimento facciale, prima di essere registrati in una banca dati istituita a tale scopo. Questi sistemi di trattamento di dati biometrici sarebbero illegali a meno che tutti gli altri ospiti monitorati (al fine di identificare i VIP) abbiano acconsentito al trattamento ai sensi dell'articolo 9, paragrafo 2, lettera a), del RGPD.

Esempio Un titolare del trattamento installa un sistema di videosorveglianza con riconoscimento facciale all'ingresso della sala da concerti da lui gestita. Il titolare deve predisporre ingressi chiaramente separati: uno provvisto del sistema biometrico e uno senza (dove, ad esempio, si esegue la scansione di un biglietto). Gli ingressi dotati di dispositivi biometrici devono essere installati e resi accessibili in modo da impedire al sistema di acquisire modelli biometrici di spettatori non consenzienti.

85.

86. Infine, quando il consenso è richiesto dall'articolo 9 del RGPD, il titolare del trattamento non deve condizionare l'accesso ai propri servizi all'accettazione del trattamento biometrico. In altre parole, in particolare quando il trattamento biometrico è utilizzato a fini di autenticazione, il titolare del trattamento deve offrire una soluzione alternativa che non comporti il trattamento biometrico, senza imporre restrizioni o costi aggiuntivi all'interessato. Tale soluzione alternativa è necessaria anche per le persone che non possono rispettare i vincoli del dispositivo biometrico (registrazione o lettura dei dati biometrici impossibile, situazione di disabilità che ne rende difficile l'utilizzo, ecc.), e in previsione dell'indisponibilità del dispositivo biometrico (ad esempio, in caso di malfunzionamento del dispositivo) deve essere attuata una «soluzione di backup», limitata tuttavia a un uso eccezionale, a garanzia della continuità del servizio proposto. In casi eccezionali, potrebbe verificarsi una situazione in cui il trattamento dei dati biometrici è l'attività principale di un servizio fornito per contratto, ad esempio un museo che allestisce una mostra per dimostrare l'uso di un dispositivo di riconoscimento facciale, nel qual caso l'interessato non potrà rifiutare il trattamento dei dati biometrici se desidera partecipare alla mostra. In questo caso, il consenso richiesto ai sensi dell'articolo 9 resta valido se sono soddisfatti i requisiti di cui all'articolo 7.

5.2 Misure proposte per ridurre al minimo i rischi durante il trattamento di dati biometrici

87. Nel rispetto del principio della minimizzazione dei dati, i titolari del trattamento devono garantire che i dati estratti da un'immagine digitale per costruire un modello non saranno eccedenti e conterranno soltanto le informazioni necessarie per la finalità specificata, evitando così ogni possibile trattamento ulteriore. Occorre adottare misure per garantire che i modelli non possano essere trasferiti tra diversi sistemi biometrici.

88. È probabile che l'identificazione e l'autenticazione/la verifica richiedano la conservazione del modello da utilizzare per i successivi raffronti. Il titolare del trattamento deve valutare quale sia il luogo più appropriato per la conservazione dei dati. In un ambiente sotto controllo (corridoi delimitati o posti di controllo), i modelli devono essere conservati su un singolo dispositivo in possesso dell'utente e sotto il suo esclusivo controllo (in uno smartphone o nella carta d'identità) oppure – se necessario per scopi specifici e in presenza di esigenze oggettive – in una banca dati centralizzata in forma cifrata con una chiave segreta nota esclusivamente alla persona interessata, per impedire l'accesso non autorizzato al modello o al luogo ove viene conservato. Se il titolare del trattamento non può evitare di accedere ai

modelli, deve adottare le opportune misure per garantire la sicurezza dei dati conservati. Può, ad esempio, cifrare il modello utilizzando un algoritmo di cifratura.

89. In ogni caso, il titolare del trattamento deve prendere tutte le precauzioni necessarie per preservare la disponibilità, l'integrità e la riservatezza dei dati trattati. A tal fine, il responsabile del trattamento deve adottare, in particolare, le seguenti misure: trasmettere e conservare i dati in forma compartimentalizzata, conservare modelli biometrici e dati grezzi o dati di identità in banche dati distinte, cifrare i dati biometrici, in particolare i modelli biometrici, e definire una politica per la cifratura e la gestione delle chiavi, prevedere una misura organizzativa e tecnica per il rilevamento delle frodi, associare un codice di integrità ai dati (ad esempio, firma o codice hash) e vietare qualsiasi accesso esterno ai dati biometrici. Tali misure dovranno evolversi con il progredire delle tecnologie.

90. Inoltre, i titolari del trattamento dovrebbero procedere alla cancellazione dei dati grezzi (immagini del volto, segnali vocali, portamento, ecc.) e garantire l'efficacia di tale cancellazione. Se non esiste più una base giuridica per il trattamento, i dati grezzi devono essere cancellati. Infatti, nella misura in cui i modelli biometrici derivano da tali dati, si può ritenere che la costituzione di database contenenti questi dati potrebbe rappresentare una minaccia analoga se non addirittura maggiore (mentre non sempre è facile leggere un modello biometrico senza sapere come è stato programmato, i dati grezzi sono gli elementi costitutivi di qualsiasi modello). Nel caso in cui il titolare del trattamento debba conservare tali dati, è necessario valutare l'impiego di metodiche basate sull'applicazione di rumore additivo (come la filigrana digitale), che impedirebbero la creazione del modello. Il titolare del trattamento deve inoltre cancellare i dati biometrici e i modelli in caso di accesso non autorizzato al terminale di lettura e raffronto o al server di conservazione, e cancellare qualsiasi dato non utile ai fini di un trattamento ulteriore al termine della vita utile del dispositivo biometrico.

6 DIRITTI DELL'INTERESSATO

91. Data la natura del trattamento dei dati associato all'impiego della videosorveglianza, necessitano chiarimenti ulteriori su alcuni diritti dell'interessato a norma del RGPD. Questo capitolo non è tuttavia esaustivo in quanto tutti i diritti sanciti dal RGPD si applicano al trattamento dei dati personali tramite videosorveglianza.

6.1 Diritto di accesso

92. Un interessato ha diritto di ottenere dal titolare del trattamento la conferma o meno del fatto che i propri dati personali siano oggetto di trattamento. Per quanto riguarda la videosorveglianza, ciò significa che se nessun dato è conservato o trasferito, una volta trascorso il momento del monitoraggio in tempo reale, il titolare potrebbe soltanto comunicare che nessun dato personale è più oggetto di trattamento (oltre alle informazioni generali obbligatorie di cui all'articolo 13, si veda la *sezione 7 – Obblighi di trasparenza e informazione*). Se tuttavia i dati sono ancora in corso di trattamento al momento della richiesta (vale a dire se i dati sono conservati o trattati ininterrottamente in qualsiasi altro modo), l'interessato dovrebbe ricevere accesso e informazioni conformemente alle disposizioni dell'articolo 15.

93. Esistono, tuttavia, alcune limitazioni che in determinati casi possono trovare applicazione rispetto al diritto di accesso.

- Articolo 15, paragrafo 4, del RGPD – Ledere i diritti altrui

94. Poiché nella stessa sequenza di videosorveglianza può essere registrato un numero qualsiasi di interessati, uno screening comporterebbe un ulteriore trattamento dei dati personali di altri interessati. Se l'interessato desidera ricevere una copia del materiale (articolo 15, paragrafo 3), ciò potrebbe ledere i diritti e le libertà di altri soggetti che compaiono nella registrazione. Per evitare tale rischio, il titolare del trattamento dovrebbe quindi tenere conto del fatto che, a causa della natura intrusiva delle riprese video, in alcuni casi non dovrebbe fornire riprese video in cui siano identificabili altri interessati. Tuttavia, la protezione dei diritti di terzi non dovrebbe essere utilizzata come pretesto per impedire legittime richieste di accesso; in questi casi, il titolare del trattamento dovrebbe porre in atto misure tecniche per soddisfare la richiesta di accesso (ad esempio, modifica delle immagini tramite mascheramento o crittografia). Tuttavia, i titolari del trattamento non sono obbligati ad attuare tali misure tecniche se possono garantire in altro modo di rispondere a una richiesta ai sensi dell'articolo 15 entro il termine stabilito dall'articolo 12, paragrafo 3.

- Articolo 11, paragrafo 2, del RGPD – Il titolare del trattamento non è in grado di identificare l'interessato

95. Se nel filmato non è possibile effettuare una ricerca di dati personali (vale a dire che il titolare del trattamento probabilmente dovrebbe analizzare una grande quantità di materiale conservato per trovare l'interessato in questione), il titolare del trattamento potrebbe non essere in grado di identificare l'interessato.

96. Per questi motivi, nella sua richiesta al titolare del trattamento l'interessato dovrebbe (oltre a identificarsi anche con un documento d'identità o di persona) specificare quando – entro un lasso di tempo ragionevole in proporzione alla quantità di interessati registrati – è entrato nella zona sorvegliata. Il titolare del trattamento dovrebbe notificare preventivamente all'interessato di quali informazioni ha bisogno per poter soddisfare la richiesta. Se il titolare del trattamento può

dimostrare di non essere in grado di identificare l'interessato, ne informa quest'ultimo, ove possibile. In un caso del genere, il titolare del trattamento dovrebbe informare l'interessato nella risposta circa la zona specificamente soggetta a sorveglianza, la verifica delle telecamere in uso, ecc., in modo che l'interessato comprenda esattamente quali dei suoi dati personali possano essere stati trattati.

Esempio Qualora l'interessato richieda una copia dei propri dati personali trattati mediante videosorveglianza all'ingresso di un centro commerciale con 30 000 visitatori al giorno, deve specificare quando ha acceduto alla zona monitorata indicando una finestra di circa un'ora. Se il titolare del trattamento sta ancora trattando il materiale, dovrebbe fornirgli una copia del filmato. Se altri interessati possono essere identificati nello stesso materiale, allora quella parte del materiale deve essere anonimizzata (ad esempio sfocando la copia o parti di essa) prima che la copia sia consegnata all'interessato che ha presentato la richiesta.

Esempio Se il titolare del trattamento cancella automaticamente tutte le riprese, ad esempio entro due giorni, non sarà in grado di fornire le riprese all'interessato dopo tale lasso di tempo. Se il titolare del trattamento riceve una richiesta successivamente, l'interessato dovrebbe esserne informato di conseguenza.

97.

- Articolo 12 del RGPD – Richieste eccessive

98. In caso di richieste eccessive o manifestamente infondate da parte di un interessato, il titolare del trattamento può addebitare un contributo spese ragionevole a norma dell'articolo 12, paragrafo 5, lettera a), del RGPD, o rifiutarsi di dare seguito alla richiesta (articolo 12, paragrafo 5, lettera b), del RGPD). Il titolare del trattamento deve essere in grado di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

6.2 Diritto alla cancellazione e diritto di opposizione

6.2.1 Diritto alla cancellazione (diritto all'oblio)

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

100. Su richiesta, il titolare del trattamento è tenuto a cancellare i dati personali senza ingiustificato ritardo se sussiste una delle circostanze elencate all'articolo 17, paragrafo 1, del RGPD (e non si applica alcuna delle eccezioni elencate all'articolo 17, paragrafo 3, del RGPD). Ciò comprende l'obbligo di cancellare i dati personali quando non sono più necessari per lo scopo per cui sono stati inizialmente conservati o quando il trattamento è illecito (si veda anche la *sezione 8 – Periodi di conservazione e obbligo di cancellazione*). Inoltre, a seconda della base giuridica del trattamento, i dati personali dovrebbero essere cancellati:

- *Per quanto riguarda il consenso,* ogni volta che il consenso viene revocato (e non vi è altra base giuridica per il trattamento)
- per quanto riguarda il *legittimo interesse*:
  - ogniqualvolta l'interessato esercita il diritto di opposizione (cfr. la *sezione 6.2.2*) e non sussistano motivi legittimi cogenti e prevalenti per il trattamento, oppure
  - in caso di marketing diretto (compresa la profilazione) ogniqualvolta gli interessati si oppongono al trattamento.

101. Se il titolare del trattamento ha reso pubbliche le riprese video (ad esempio, trasmissione o streaming online), è necessario adottare misure ragionevoli per informare altri titolari (che stanno attualmente trattando i dati personali in questione) della richiesta ai sensi dell'articolo 17, paragrafo 2, del RGPD. Le misure ragionevoli dovrebbero comprendere misure tecniche che tengano conto della tecnologia disponibile e dei costi di implementazione. Nella misura del possibile, il titolare del trattamento dovrebbe informare – in caso di cancellazione dei dati personali – qualunque soggetto al quale siano stati precedentemente comunicati tali dati, conformemente a quanto disposto nell'articolo 19 del RGPD.

102. Oltre all'obbligo di cancellare i dati personali su richiesta dell'interessato, il titolare del trattamento è tenuto, in virtù dei principi generali del RGPD, a limitare i dati personali conservati (si veda la *sezione 8*).

103. Rispetto alla videosorveglianza vale la pena osservare, ad esempio, che offuscando l'immagine senza alcuna possibilità di recuperare successivamente i dati personali precedentemente contenuti in tale immagine , si deve ritenere che i dati personali siano stati cancellati in conformità delle disposizioni del RGPD.

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

104.

6.2.2 Diritto di opposizione

105. Rispetto alla videosorveglianza basata su un *legittimo interesse* (articolo 6, paragrafo 1, lettera f), del RGPD), o con riguardo alla necessità nello svolgimento di un compito di *interesse pubblico* (articolo 6, paragrafo 1, lettera e), del RGPD) l'interessato ha il diritto di opporsi al trattamento in qualsiasi momento, per motivi connessi alla sua situazione particolare, ai sensi dell'articolo 21 del RGPD. A meno che il titolare del trattamento possa dimostrare l'esistenza di motivi legittimi cogenti che prevalgono sui diritti e sugli interessi dell'interessato, il trattamento dei dati della persona che vi si è opposta deve cessare. Il titolare è tenuto a rispondere alle richieste dell'interessato senza ingiustificato ritardo e al più tardi entro un mese.

106. Nel contesto della videosorveglianza, tale opposizione potrebbe essere formulata all'ingresso, durante il periodo di permanenza nella zona sorvegliata o dopo l'uscita dalla stessa. In pratica ciò significa che, a meno che il titolare del trattamento abbia motivi legittimi cogenti, la sorveglianza di una zona in cui potrebbero essere identificate persone fisiche è lecita unicamente se:

(1) il titolare è in grado di interrompere immediatamente, su richiesta, il trattamento dei dati personali da parte della telecamera, o

(2) la zona sorvegliata è soggetta a restrizioni tali da consentire al titolare del trattamento di ottenere il consenso dell'interessato prima che questi vi acceda e non è una zona a cui l'interessato in quanto cittadino ha diritto di accedere.

107. Le presenti linee guida non mirano a identificare ciò che è considerato un legittimo interesse *cogente* (articolo 21 del RGPD).

108. Quando si utilizza la videosorveglianza per finalità di marketing diretto, l'interessato ha il diritto di opporsi al trattamento a sua discrezione; il diritto di opposizione, infatti, è assoluto in tale contesto (articolo 21, paragrafi 2 e 3, del RGPD).

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

109.

7 OBBLIGHI DI TRASPARENZA E INFORMAZIONE ([18])

110. La normativa europea in materia di protezione dei dati dispone da tempo che gli interessati debbano essere consapevoli del fatto che è in funzione un sistema di videosorveglianza. Dovrebbero essere informati in modo dettagliato sui luoghi sorvegliati ([19]). A norma del RGPD gli obblighi generali di trasparenza e informazione sono sanciti dall'articolo 12 e seguenti del RGPD. Le «Linee guida sulla trasparenza ai sensi del regolamento (UE) 2016/679 (WP260)» del gruppo di lavoro "Articolo 29", approvate dal comitato europeo per la protezione dei dati il 25 maggio 2018, forniscono ulteriori dettagli. In linea con il punto 26 del WP260, è l'articolo 13 del RGPD che si applica se i dati personali sono raccolti «[…] presso l'interessato mediante osservazione (ad es. utilizzando dispositivi o software per catturare dati in modo automatizzato quali telecamere, […])».

111. Alla luce della quantità di informazioni da fornire all'interessato, i titolari del trattamento possono seguire un approccio scalare, optando per una combinazione di metodi al fine di assicurare la trasparenza (WP260, punto 35; WP89, punto 22). Per quanto riguarda la videosorveglianza, le informazioni più importanti devono essere indicate sul segnale di avvertimento stesso (primo livello), mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello).

7.1 Informazioni di primo livello (segnaletica di avvertimento)

112. Il primo livello riguarda la modalità con cui avviene la prima interazione fra il titolare del trattamento e l'interessato. In questa fase, i titolari del trattamento possono utilizzare un segnale di avvertimento che indichi le informazioni pertinenti. Tali informazioni possono essere fornite in combinazione con un'icona per dare, in modo ben visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto (articolo 12, paragrafo 7, del RGPD). Il formato delle informazioni dovrà adeguarsi alle varie ubicazioni (WP89, punto 22).

7.1.1 Posizionamento della segnaletica di avvertimento

113. Le informazioni dovrebbero essere posizionate in modo da permettere all'interessato di riconoscere facilmente le circostanze della sorveglianza, prima di entrare nella zona sorvegliata (approssimativamente all'altezza degli occhi). Non è necessario rivelare l'ubicazione della telecamera, purché non vi siano dubbi su quali zone sono soggette a sorveglianza e sia chiarito in modo inequivocabile il contesto della sorveglianza (WP 89, punto 22). L'interessato deve poter stimare quale zona sia coperta da una telecamera in modo da evitare la sorveglianza o adeguare il proprio comportamento, ove necessario.

7.1.2 Contenuto delle informazioni di primo livello

114. Generalmente, le informazioni di primo livello (segnale di avvertimento) dovrebbero comunicare i dati più importanti, ad esempio le finalità del trattamento, l'identità del titolare del trattamento e l'esistenza dei diritti dell'interessato, unitamente alle informazioni sugli impatti più consistenti del trattamento ([20]). Si può fare riferimento, ad esempio, ai legittimi interessi perseguiti dal titolare (o da un soggetto terzo) e ai recapiti del responsabile della protezione dei dati (se applicabile). Occorre

([18]) Potrebbero essere applicabili disposizioni specifiche della normativa nazionale.

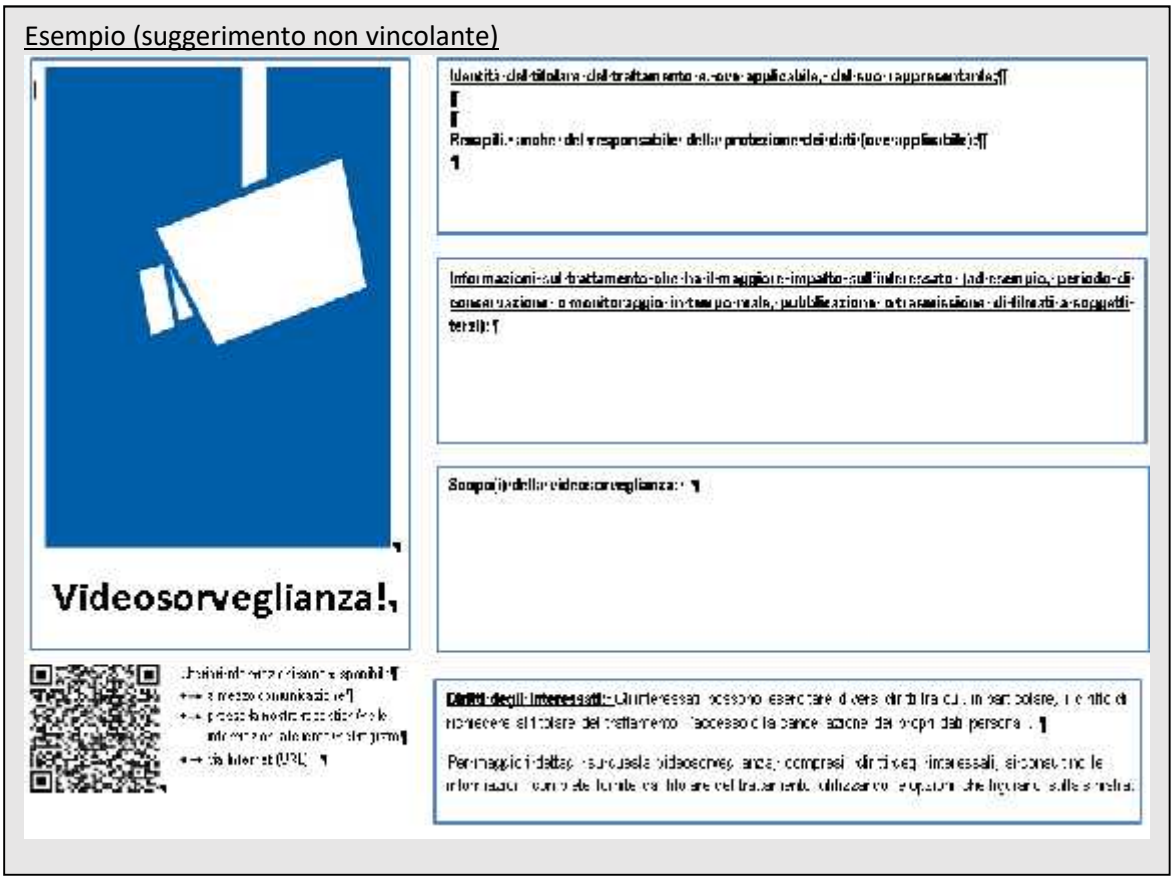
([19]) Cfr. il WP89, parere 4/2004 relativo al trattamento dei dati personali mediante videosorveglianza del gruppo di lavoro dell'articolo 29).

[20] Cfr. il WP260, punto 38.

anche fare riferimento alle informazioni di secondo livello, più dettagliate,, indicando dove e come trovarle.

115. Inoltre, la segnaletica deve contenere anche quelle informazioni che potrebbero risultare inaspettate per l'interessato (WP260, punto 38). Potrebbe trattarsi, ad esempio, della trasmissione di dati a terzi, in particolare se ubicati al di fuori dell'UE, e del periodo di conservazione. Se tali informazioni non sono indicate, l'interessato dovrebbe poter confidare nel fatto che vi sia solo una sorveglianza in tempo reale (senza alcuna registrazione di dati o trasmissione a soggetti terzi).

Esempio (suggerimento non vincolante)



116.

7.2 Informazioni di secondo livello

117. Le informazioni di secondo livello devono essere facilmente accessibili per l'interessato, ad esempio attraverso un pagina informativa completa messa a disposizione in uno snodo centrale (sportello informazioni, reception, cassa, ecc.) o affissa in un luogo di facile accesso. Come sopra illustrato, la segnaletica di avvertimento di primo livello deve contenere un chiaro riferimento a tale secondo livello di informazioni. Inoltre, è preferibile che nelle informazioni di primo livello si faccia riferimento a una fonte digitale (ad esempio, un codice QR o un indirizzo web) per le informazioni di secondo livello. Tuttavia, le informazioni dovrebbero essere facilmente disponibili anche in formato non digitale. Dovrebbe essere possibile accedere al secondo livello di informazioni senza entrare nell'area videosorvegliata, soprattutto se le informazioni sono fornite digitalmente (ad esempio, tramite un link). Un altro strumento appropriato potrebbe essere la messa a disposizione di un numero telefonico da contattare. Comunque siano fornite le informazioni, queste devono contenere tutti gli elementi obbligatori a norma dell'articolo 13 del RGPD.

118. Oltre a queste possibilità, e anche per renderle più efficaci, il comitato europeo per la protezione dei dati promuove l'uso di strumenti tecnologici per fornire informazioni agli interessati. Per esempio, si possono geolocalizzare le telecamere caricando le relative informazioni su app o siti web di mappatura, cosicché le persone possano facilmente, da un lato, identificare e specificare le fonti video in vista dell'esercizio dei propri diritti e, dall'altro lato, ottenere informazioni più dettagliate sulla tipologia di trattamento.

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

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 RGPD). In alcuni Stati membri possono essere previste disposizioni specifiche per i periodi di conservazione con riguardo alla videosorveglianza a norma dell'articolo 6, paragrafo 2, del RGPD.

121. La necessità o meno di conservare i dati personali dovrebbe essere valutata entro una tempistica ristretta. In via generale, gli scopi legittimi della videosorveglianza sono spesso la protezione del patrimonio o la conservazione di elementi di prova. Solitamente è possibile individuare eventuali danni entro uno o due giorni. Per facilitare la dimostrazione di conformità al quadro normativo in materia di protezione dei dati, è nell'interesse del titolare del trattamento organizzarsi proattivamente (ad esempio nominando, se necessario, un responsabile per lo screening e la protezione del materiale video). Tenendo conto dei principi di cui all'articolo 5, paragrafo 1, lettere c) ed e), del RGPD, vale a dire la minimizzazione dei dati e la limitazione della loro conservazione, i dati personali dovrebbero essere – nella maggior parte dei casi (ad esempio se la videosorveglianza serve allo scopo di rilevare atti vandalici) – cancellati dopo alcuni giorni, preferibilmente tramite meccanismi automatici. Quanto più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione. Se il titolare del trattamento utilizza la videosorveglianza non solo per monitorare i propri locali, ma anche per conservare i dati, deve garantire che la conservazione sia effettivamente necessaria per raggiungere lo scopo specifico. In tal caso, il periodo di conservazione deve essere definito chiaramente e specificamente con riguardo alle singole finalità. È responsabilità del titolare del trattamento definire il periodo di conservazione conformemente ai principi di necessità e proporzionalità e dimostrare la conformità alle disposizioni del RGPD.

> Esempio Normalmente, il titolare di un piccolo esercizio commerciale si accorgerebbe di eventuali atti vandalici il giorno stesso in cui si verificassero. Un periodo di conservazione di 24 ore è quindi sufficiente. La chiusura nei fine settimana o in periodi festivi più lunghi potrebbe tuttavia giustificare un periodo di conservazione più prolungato. Se viene rilevato un danno, può essere anche necessario conservare il filmato per un periodo più lungo al fine di intraprendere un'azione legale contro l'autore del reato.

122.

9 MISURE TECNICHE E ORGANIZZATIVE

123. Come indicato all'articolo 32, paragrafo 1, del RGPD, non è sufficiente che il trattamento di dati personali durante videosorveglianza sia lecito, in quanto titolari e responsabili del trattamento devono anche garantire l'adeguata sicurezza dei dati in questione . **Le misure tecniche** e **organizzative** attuate devono essere **proporzionate ai rischi per i diritti e le libertà delle persone fisiche** derivanti dai casi di distruzione accidentale o illecita, perdita, alterazione, divulgazione non autorizzata o accesso ai dati di videosorveglianza. A norma degli articoli 24 e 25 del RGPD, i titolari del trattamento devono mettere in atto misure tecniche e organizzative anche al fine di salvaguardare tutti i principi di protezione dei dati durante il trattamento e di stabilire i mezzi affinché gli interessati possano esercitare i propri diritti secondo la definizione di cui agli articoli 15-22 del RGPD. I titolari del trattamento dovrebbero adottare una struttura interna e politiche in grado di assicurare l'attuazione di tali misure sia al momento di definire i mezzi di trattamento sia all'atto del trattamento stesso, compresa l'esecuzione di valutazioni d'impatto sulla protezione dei dati ove necessario.

9.1 Descrizione generale di un sistema di videosorveglianza

124. Un sistema di videosorveglianza (VSS) ([21]) è costituito da dispositivi analogici e digitali nonché da software per acquisire immagini, gestirle e mostrarle a un operatore. I suoi componenti sono categorizzabili come segue:

- Ambiente video: acquisizione immagini, interconnessioni e gestione immagini:
  - l'acquisizione delle immagini serve a generare un'immagine del mondo reale in un formato tale da poter essere utilizzata dal resto del sistema,
  - le interconnessioni comprendono tutte le trasmissioni di dati all'interno dell'ambiente video, vale a dire connessioni e comunicazioni. Esempi di connessioni sono cavi, reti digitali e trasmissioni wireless. Le comunicazioni descrivono tutti i segnali video e dati di controllo, che potrebbero essere digitali o analogici,
  - la gestione delle immagini comprende l'analisi, la conservazione 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 delle attività, comprendente la gestione dei comandi degli operatori e delle attività generate dal sistema (procedure di allarme, operatori di allarme),
  - le interfacce con altri sistemi potrebbero includere la connessione ad altri sistemi di sicurezza (controllo accessi, allarme antincendio) o non legati alla sicurezza (sistemi di gestione edifici, riconoscimento automatico delle targhe).
- La sicurezza di un VSS consiste nella riservatezza, nell'integrità e nella 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]) Il RGPD non definisce i sistemi di videosorveglianza; una descrizione tecnica è disponibile ad esempio nella norma EN 62676-1-1:2014 Sistemi di videosorveglianza per l'uso in applicazioni di sicurezza – Parte 1-1: requisiti del sistema video

125.

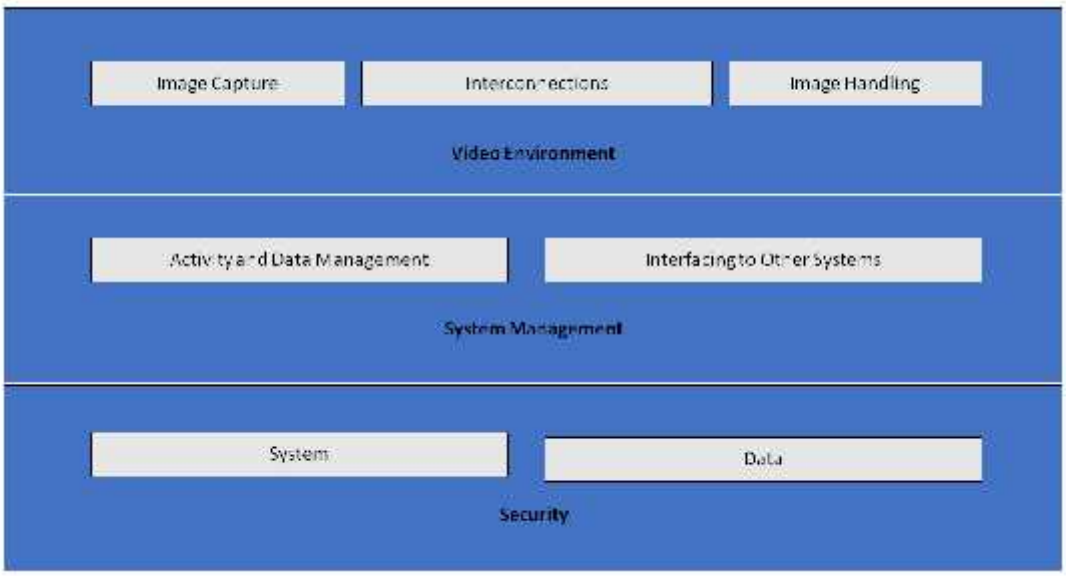


Image Capture	Acquisizione immagini
Interconnections	Interconnessioni
Image Handling	Gestione immagini
Video Environment	Ambiente video
Activity and Data Management	Gestione dell'attività e dei dati
Interfacing to Other Systems	Interfacciamento con altri sistemi
System Management	Gestione del sistema
System	Sistema
Data	Dati
Security	Sicurezza

Figura 1. Sistema di videosorveglianza

9.2 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

126. Come stabilito dall'articolo 25 del RGPD, i titolari del trattamento devono mettere in atto adeguate misure tecniche e organizzative di protezione dei dati non appena pianificano l'installazione di un sistema di videosorveglianza, prima di iniziare la raccolta e il trattamento di filmati. Questi principi sottolineano la necessità di tecnologie integrate per il miglioramento della privacy, impostazioni predefinite che riducano al minimo il trattamento dei dati e l'adozione degli strumenti necessari ai fini della massima protezione possibile dei dati personali ([22]).

127. I titolari 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. Per quanto riguarda queste ultime, il titolare del trattamento dovrebbe adottare un piano di gestione appropriato, 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 conformemente ai principi di cui all'articolo 5 del RGPD (liceità del trattamento, limitazione

([22]) WP 168, Parere sul tema «Il futuro della privacy», contributo congiunto del gruppo di lavoro "Articolo 29" 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 1º dicembre 2009).

della finalità e dei dati, minimizzazione dei dati per impostazione predefinita ai sensi dell'articolo 25, paragrafo 2, del RGPD, integrità e riservatezza, responsabilizzazione, ecc.). Nel caso in cui un titolare del trattamento preveda di acquistare un sistema di videosorveglianza commerciale, deve includere questi requisiti nelle specifiche di acquisto. Il titolare del trattamento deve garantire la conformità a questi requisiti, applicandoli a tutti i componenti del sistema e a tutti i dati da esso trattati, durante l'intero ciclo di vita.

9.3 Esempi concreti di misure pertinenti

128. La maggior parte delle misure che possono essere utilizzate per la sicurezza dei trattamenti di videosorveglianza, soprattutto quando si utilizzano apparecchiature digitali e software, sono sostanzialmente identiche alle misure utilizzate in altri sistemi informatici. Tuttavia, indipendentemente dalla soluzione prescelta, il titolare del trattamento deve proteggere adeguatamente tutti i componenti di un sistema di videosorveglianza e i dati in tutte le fasi, vale a dire durante la conservazione (dati a riposo), la trasmissione (dati in transito) e il trattamento (dati in uso). A tal fine è necessario che titolari e responsabili del trattamento combinino misure organizzative e tecniche.

129. Nel selezionare le soluzioni tecniche, il titolare del trattamento dovrebbe considerare le tecnologie che tutelano la privacy anche perché migliorano la sicurezza. Esempi di questo tipo di tecnologie sono i sistemi che consentono il mascheramento o l'offuscamento delle zone irrilevanti per la sorveglianza, oppure l'editing di immagini di terzi, quando si forniscono filmati agli interessati ([23]). D'altra parte, le soluzioni individuate non dovrebbero prevedere funzioni non necessarie (ad esempio, movimento illimitato delle telecamere, capacità di zoom, radiotrasmissione, analisi e registrazioni audio). Le funzioni fornite, ma non necessarie, devono essere disattivate.

130. Su questo argomento è disponibile una vasta letteratura, comprese le norme internazionali e le specifiche tecniche sulla sicurezza fisica dei sistemi multimediali ([24]) e sulla sicurezza dei sistemi informatici ([25]) in genere. Questa sezione fornisce quindi una panoramica di alto livello di questo argomento.

9.3.1 Misure organizzative

131. Oltre alla eventuale necessità di una valutazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment*, DPIA) (si veda la *sezione 10*), nell'elaborare le proprie politiche e procedure di videosorveglianza i titolari del trattamento dovrebbero prendere in considerazione gli elementi indicati di seguito.

- Responsabilità della gestione e del funzionamento del sistema di videosorveglianza.
- Finalità e ambito di applicazione del progetto di videosorveglianza.

([23]) L'uso di tali tecnologie può anche essere obbligatorio in alcuni casi al fine di osservare le disposizioni di cui all'articolo 5, paragrafo 1, lettera c). In ogni caso, può servire da esempio di buone prassi.

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

([25]) ISO/IEC 27000:2013 – Sistemi di gestione per la sicurezza delle informazioni.

- Utilizzo appropriato e vietato (dove e quando la videosorveglianza è consentita e dove e quando non lo è: ad esempio, uso di telecamere nascoste e registrazione audio oltre che video) ([26]).
- Misure di trasparenza di cui alla *sezione 7 (Obblighi di trasparenza e informazione).*
- Modalità e durata delle registrazioni video, compresa la conservazione delle videoregistrazioni relative a problemi di sicurezza.
- Chi deve seguire una formazione specifica e quando.
- Chi ha accesso alle registrazioni video e per quali scopi.
- Procedure operative (ad esempio, da chi e da dove viene monitorata la videosorveglianza, cosa fare in caso di un problema di violazione dei dati).
- Quali procedure devono seguire i soggetti esterni per richiedere le videoregistrazioni e le procedure per respingere o accogliere tali richieste.
- Procedure per l'approvvigionamento, l'installazione e la manutenzione di VSS.
- Gestione dei problemi e procedure di recupero.

9.3.2 Misure tecniche

132. **Sicurezza del sistema** significa **sicurezza fisica** di tutti i componenti del sistema, nonché integrità del sistema, vale a dire **protezione e resilienza in caso di interferenze volontarie e involontarie nel suo normale funzionamento** e **controllo degli accessi**. Sicurezza dei dati significa **riservatezza** (i dati sono accessibili solo a coloro a cui è concesso l'accesso), **integrità** (prevenzione della perdita o della manipolazione dei dati) e **disponibilità** (i dati possono essere consultati ogniqualvolta sia necessario).

133. La **sicurezza fisica** è una parte fondamentale della protezione dei dati e costituisce la prima linea di difesa, perché protegge le apparecchiature VSS da furti, atti vandalici, calamità naturali, catastrofi provocate dall'uomo e danni accidentali (ad esempio, sovratensioni elettriche, temperature estreme e riversamento di caffè). Nel caso di sistemi analogici, la sicurezza fisica è la più importante per la loro protezione.

134. La **sicurezza del sistema e dei dati**, vale a dire la protezione da interferenze volontarie e involontarie nel suo normale funzionamento, può comprendere:

- protezione dell'intera infrastruttura del VSS (comprese telecamere remote, cablaggio e alimentazione) contro manomissioni fisiche e furti;
- protezione della trasmissione di filmati attraverso canali di comunicazione sicuri a prova di intercettazione;
- cifratura dei dati;
- utilizzo di soluzioni basate su hardware e software quali firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici;
- rilevamento di guasti di componenti, software e interconnessioni;
- strumenti per ripristinare la disponibilità dei dati personali e l'accesso agli stessi in caso di problemi fisici o tecnici.

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

([26]) Ciò può dipendere dalle leggi nazionali e dalle normative settoriali.

- la garanzia che tutti i locali in cui viene effettuato il monitoraggio mediante videosorveglianza e in cui vengono conservate le riprese video siano protetti contro l'accesso non supervisionato da parte di terzi;
- il posizionamento dei monitor (soprattutto quando si trovano in zone aperte, come una reception) in modo tale che solo gli operatori autorizzati possano visualizzarli;
- la definizione e l'applicazione delle procedure per la concessione, la modifica e la revoca dell'accesso;
- l'attuazione di metodi e mezzi di autenticazione e autorizzazione dell'utente, tra cui ad esempio la lunghezza delle password e la frequenza della loro modifica;
- la registrazione e la revisione periodica delle azioni eseguite dagli utenti (con riguardo sia al sistema sia ai dati);
- l'esecuzione del monitoraggio e l'individuazione di guasti agli accessi in modo continuativo e la risoluzione in tempi brevi delle carenze individuate.

10 VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

136. Ai sensi dell'articolo 35, paragrafo 1, del RGPD, i titolari del trattamento sono tenuti a condurre valutazioni d'impatto sulla protezione dei dati quando una determinata tipologia di trattamenti può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. L'articolo 35, paragrafo 3, lettera c), del RGPD stabilisce che i titolari del trattamento sono tenuti a effettuare valutazioni d'impatto sulla protezione dei dati se il trattamento consiste nella sorveglianza sistematica di una zona accessibile al pubblico su larga scala. Inoltre, ai sensi dell'articolo 35, paragrafo 3, lettera b), del RGPD, è necessaria una valutazione d'impatto sulla protezione dei dati anche quando il titolare intende trattare categorie particolari di dati su larga scala.

137. Le linee guida in materia di valutazione d'impatto sulla protezione dei dati ([27]) forniscono ulteriori indicazioni ed esempi più dettagliati relativi alla videosorveglianza (ad esempio, per quanto riguarda «l'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade»). L'articolo 35, paragrafo 4, del RGPD prevede che ogni autorità di controllo pubblichi un elenco delle tipologie di trattamento soggette obbligatoriamente a valutazione d'impatto sulla protezione dei dati nel rispettivo Stato membro. Di norma, questi elenchi sono reperibili sui siti web delle autorità. Date le finalità tipiche della videosorveglianza (protezione delle persone e dei beni, individuazione, prevenzione e controllo di reati, raccolta di elementi di prova e identificazione biometrica di soggetti sospetti), è ragionevole supporre che molti casi di videosorveglianza richiederanno una valutazione d'impatto sulla protezione dei dati. I titolari del trattamento dovrebbero quindi consultare attentamente questi documenti al fine di determinare se tale valutazione sia necessaria e, in tal caso, al fine di effettuarla. L'esito della valutazione d'impatto sulla protezione dei dati dovrebbe determinare la scelta del titolare del trattamento sulle misure di protezione dei dati implementate.

138. È inoltre importante ricordare che, ove i risultati della valutazione d'impatto sulla protezione dei dati indichino che il trattamento comporterebbe un rischio elevato nonostante le misure di sicurezza pianificate dal titolare, occorrerà consultare l'autorità di controllo competente prima di procedere al trattamento. Le disposizioni in materia di consultazioni preventive sono contenute nell'articolo 36 del RGPD.

Per il comitato europeo per la protezione dei dati

La presidente

(Andrea Jelinek)

([27]) WP 248 rev.01, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento «possa presentare un rischio elevato» ai fini del regolamento (UE) 2016/679 – approvate dal Comitato europeo per la protezione dei dati.