DPO – Parere del 11.08.2020

Multibusiness srl - Responsabile Protezione Dati

RPARERE SU AUTORIZZAZIONE RILASCIO COPIA DI REGISTRAZIONE TELECAMERE

Responsabile della Protezione dei Dati (RPD/DPO)

Il presente Parere tiene conto dell'art. 38, paragrafo 3, del GDPR, che prevede che il Responsabile della Protezione dei Dati/Data Protection Officer (RPD/DPO) "**riferisce direttamente al vertice gerarchico del Titolare del trattamento o a soggetti dallo stesso individuati**".

A seguito dell'affidamento dell'incarico quale Responsabile della Protezione dei Dati (RPD/DPO) e servizi finalizzati all'adeguamento alla vigente normativa, in riscontro a Vs mail di richiesta parere, si espone quanto segue:

SOMMARIO

PREMESSA

Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza non trova legislazione specifica; al riguardo **si applicano**, pertanto, le disposizioni generali in tema di protezione dei dati personali, in particolare **il provvedimento dell'autorità garante per la protezione dei dati personali dell'8 aprile 2010 in materia di videosorveglianza** (che ovviamente non tiene conto del GDPR, essendo stato emanato prima della sua entrata in vigore), e **Le linee guida in materia di videosorveglianza del Comitato Europeo per la Protezione dei Dati** (che ha sostituito il WP articolo 29), al contrario redatte alla luce del Regolamento Europeo 679/2016 (d'ora in poi "GDPR").

Più precisamente, al punto 4, le Linee Guida prendono in esame la delicata situazione **della comunicazione a terzi e della diffusione di filmati acquisiti con le telecamere di sorveglianza**.

Com'è noto, in primis il GDPR, e di conseguenza le linee guida dell'European Data Protection Board (d'ora in poi semplicemente EDPB), non contengono prescrizioni in senso stretto, bensì una lettura integrativa delle disposizioni del GDPR, quindi **di carattere interpretativo**, servono a guidare, precisare, esemplificare.

Perché sono state emanate le Linee guida sulla videosorveglianza

L'EDPB prende atto della massiccia diffusione di impianti/apparecchiature di videosorveglianza e, con essa, del fatto che queste tecnologie "possono limitare le possibilità di movimento e di utilizzo anonimo dei servizi" e, in generale, la possibilità di passare inosservati, per cui "le implicazioni per la protezione dei dati sono enormi".

*Per questo la videosorveglianza non è da considerare automaticamente una necessità, quando siano disponibili altri mezzi per raggiungere lo scopo sottostante.

Campo di applicazione, basi giuridiche, bilanciamento degli interessi

È utile ricordare che il **GDPR** non si applica ai trattamenti di dati:

→ che non hanno alcun riferimento a una persona, in quanto non identificata e neppure identificabile;

→ eseguiti da parte delle autorità competenti ai fini della prevenzione, delle indagini, dell'accertamento o del perseguimento di reati o dell'esecuzione di sanzioni penali, compresa la tutela e la prevenzione di minacce alla sicurezza pubblica (poiché ambito di riserva della Direttiva UE 2016/680);

→ da parte di una persona fisica nell'ambito di un'attività puramente personale o domestica.

Basi giuridiche su cui si fonda/basa il trattamento (art. 6.1 del GDPR)

Il trattamento **è lecito solo se** e nella misura in cui ricorre **almeno una** delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Il EDPB ritiene che qualsiasi fattispecie di cui all'art. 6.1 possa costituire la base giuridica di un trattamento mediante videosorveglianza. Tuttavia, scendendo dalla teoria alla pratica, le basi giuridiche più ricorrenti sono **il legittimo interesse** (art. 6.1, lett. f) e la necessità dell'**esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** (art. 6.1, lett. e).

**Al consenso (art. 6.1, lett. a) è destinato uno spazio residuale, ipotesi "piuttosto eccezionali".*

L'identificazione biometrica

Uno degli argomenti più delicati, anche per effetto dell'evoluzione dei sistemi di videosorveglianza, è quello della **identificazione biometrica** degli interessati attraverso l'analisi degli elementi del viso. È fondamentale che il ricorso a tali tecnologie avvenga NEL RISPETTO dei **principi di liceità, necessità, proporzionalità e minimizzazione dei dati** stabiliti nel GDPR, poiché l'uso di tali tecnologie può essere facilmente distorto e consentire abusi da parte del titolare che deve sempre tenere presente la regola secondo la quale un determinato trattamento è ammesso SOLO SE non ve ne sono di alternativi, meno impattanti sui diritti e sulle libertà dell'interessato, che permettono di perseguire le stesse finalità con pari efficacia.

I criteri della definizione

Le Linee guida chiariscono anche che non è sufficiente la possibile identificazione dell'interessato per richiamare la biometria come elemento di valutazione in negativo del trattamento, poiché per identificazione biometrica si intende il risultato di una specifica tecnica di elaborazione delle ".. caratteristiche fisiche, psicologiche o comportamentali dell'individuo..".

Alla luce degli artt. 4 e 9 del GDPR, sono necessari **tre criteri** per poter parlare di identificazione biometrica:

1) l'individuazione di una o più caratteristiche fisiche, psicologiche o comportamentali dell'interessato;
2) un procedimento tecnico di rilevazione e trattamento di tali caratteristiche;
3) un procedimento di elaborazione del dato (creazione del database o confronto con il database già esistente) che permetta l'identificazione univoca dell'interessato.

***N.B.:** L'uso di un sistema di rilevazione biometrica di questo tipo, **da parte di un soggetto privato**, è sempre subordinato al consenso dell'interessato.

DIRITTI DELL'INTERESSATO

Diritto di accesso

L'interessato ha **diritto di ottenere** dal Titolare del trattamento la conferma dell'esistenza o meno di propri dati personali.

Per la videosorveglianza ciò significa che se nessun dato viene memorizzato o trasferito in alcun modo, una volta trascorso il momento di monitoraggio in tempo reale, il Titolare può solo dare l'informazione che nessun dato personale è più oggetto di trattamento.

Se i dati **sono ancora in corso di trattamento al momento della richiesta** (cioè se i dati sono memorizzati o trattati in modo continuativo in qualsiasi altro modo), l'interessato deve ricevere accesso e informazioni, ai sensi del richiamato articolo 15. Vi sono tuttavia **alcune limitazioni** che in alcuni casi possono essere applicate in relazione al diritto di accesso.

- Articolo 15, paragrafo 4, pregiudica i diritti altrui

Dato che un numero qualsiasi di soggetti interessati **può essere registrato nella stessa sequenza di videosorveglianza**, una proiezione provocherebbe un ulteriore trattamento dei dati personali di altri soggetti. Se l'interessato (o un soggetto da esso delegato) **desidera ricevere una copia del materiale** (articolo 15, paragrafo 3), ciò potrebbe pregiudicare i diritti e le libertà degli altri

interessati. Per evitare tale effetto **il Titolare** del trattamento **deve** pertanto **tenere conto** del fatto **che**, a causa della natura intrusiva dei filmati, **in alcuni casi non deve distribuire filmati in cui siano identificabili altri soggetti**.

La tutela dei diritti di terzi NON DEVE tuttavia essere utilizzata come pretesto per impedire legittime rivendicazioni di accesso da parte di persone fisiche; in questi casi **IL TITOLARE DEL TRATTAMENTO DEVE ATTUARE MISURE TECNICHE PER SODDISFARE LA RICHIESTA DI ACCESSO** (ad esempio, la modifica delle immagini come il mascheramento).

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

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

Per tali ragioni **l'interessato dovrebbe** (OLTRE AD IDENTIFICARSI ANCHE CON DOCUMENTO DI IDENTITÀ O DI PERSONA) **nella sua richiesta**, **specificare quando** - entro un ragionevole lasso di tempo in proporzione alla quantità di dati registrati - **è entrato nell'area monitorata**. * Il Titolare del trattamento deve comunicare preventivamente all'interessato le informazioni necessarie affinché possa soddisfare la richiesta.

Se il Titolare del trattamento è in grado di dimostrare di non essere in grado di identificare l'interessato, deve informare l'interessato di conseguenza, se possibile. In tale situazione, nella sua risposta all'interessato, il titolare del trattamento deve informare l'interessato sull'area esatta per il monitoraggio, la verifica delle telecamere che erano in uso, ecc. in modo che l'interessato abbia la piena comprensione di quali dati personali possono essere stati trattati.

RICHIESTE ECCESSIVE

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

ALTRA FATTISPECIE: NOTE SUL CODICE DELLA STRADA

Modalità da seguire per gli accessi agli atti

L'articolo 11, comma 4, del C.d.S. consente agli interessati in relazione ad un incidente stradale di chiedere agli organi di polizia che in concerto hanno svolto il servizio di rilevazione dell'incidente informazioni concernenti: "le modalità dell'incidente, la residenza ed il domicilio delle parti, la copertura assicurativa dei veicoli ed i dati di individuazione di questi ultimi".

In attuazione della citata disposizione del C.d.S., e in base alla regolamentazione dell'Ente:

a. quanto alla richiesta di informazione, ne è titolare il soggetto che sia interessato comunque (vittima o autore o responsabile civile) ad un determinato incidente stradale. La richiesta stessa va presentata direttamente al protocollo del comune oppure inviata (tramite raccomandata con ricevuta di ritorno o PEC alla Polizia Locale;

b. è previsto l'obbligo dell'Ufficio destinatario di fornire le informazioni richieste, seguendo la procedura ordinaria vigente in tale materia.

Particolari cautele sono previste nel caso in cui dall'incidente possa derivare un ***reato***:

- se questo è perseguibile d'ufficio (omicidio colposo) occorre la previa autorizzazione dell'Autorità Giudiziaria (che certamente terrà conto dello stato del procedimento penale);
- se il reato è perseguibile a querela (lesioni colpose) occorre, se il procedimento è pendente (e quindi la querela è stata presentata) la previa autorizzazione dell'Autorità Giudiziaria, ovvero, se il procedimento penale non è in corso, l'attestazione, rilasciata dalla stessa Autorità ed esibita dal richiedente, dell'avvenuto decorso del termine di legge per la presentazione della querela.

IL CASO CONCRETO

La divulgazione dei dati/immagini/video

Con il termine divulgazione si allude nelle Linee guida **SIA** alla comunicazione **CHE** alla diffusione dei dati. Per esse dovrà essere definita, di volta in volta, la base giuridica adeguata all'eventuale ulteriore trattamento.

IL LEGITTIMO INTERESSE: Titolare e interessato, un bilanciamento delicato

Particolare attenzione è dedicata al legittimo interesse (che è la base giuridica su cui si fonda il caso da voi prospettato), che potrà dirsi correttamente richiamato e invocato allorché sia stata **preventivamente e scrupolosamente valutata la sua prevalenza sugli interessi, i diritti e le libertà degli interessati**; valutazione da compiere mai in astratto, ma **caso per caso** (NELLA CIRCOSTANZA L'INTERESSATO IL DOTT. ANTONIO MARIA SORU, PER MEZZO DEL SUO LEGALE, DICHIARA DI ESSERE PROPRIETARIO DI UN'AUTOVETTURA COINVOLTA IN UN SINISTRO, QUINDI VANTA UN LEGITTIMO INTERESSE DI TUTELA NEI CONFRONTI DI TERZI).

Questo interesse deve essere **reale e attuale** e potrà anche essere giustificato da fatti/incidenti accaduti che, nel caso, è consigliato al Titolare di **documentare** le valutazioni e decisioni prese

(NEL CASO SPECIFICO L'INTERESSE VANTATO È REALE E ATTUALE. INOLTRE QUESTE NOSTRE CORRISPONDENZE SONO "DOCUMENTAZIONI" DELLE DECISIONI DA VOI PRESE RELATIVAMENTE ALLA RICHIESTA DI RILASCIO DELLE COPIE).

ESEMPIO
Per esempio, risulta giustificata la trasmissione a un avvocato delle immagini di un danneggiamento, rilevate dalle telecamere installate in un parcheggio, perché l'azione promossa per ottenere il risarcimento del danno è la logica prosecuzione della finalità di tutela del patrimonio che ha motivato l'installazione dell'impianto di videosorveglianza.

COLLABORARE CON LE FORZE DELL'ORDINE È UN OBBLIGO

Un altro argomento preso in esame dalle valutazioni dell'EDPB è quello della consegna dei filmati delle telecamere alle Forze dell'Ordine. L'EDPB ribadisce il principio secondo il quale è un **obbligo di legge collaborare** con le Forze dell'Ordine e la Magistratura ed è quindi **sempre giustificata** la cessione dei filmati acquisiti dalle telecamere secondo le norme procedurali che regolano l'attività di indagine della polizia giudiziaria.

ESEMPIO
Per esempio, nel caso di un crimine avvenuto nelle immediate vicinanze di un'azienda che ha un impianto di videosorveglianza posizionato anche all'esterno della recinzione, le Forze dell'Ordine intervenute possono chiedere al titolare di esportare le immagini dalle memorie e consegnarle al fine di utilizzarle nell'instaurando procedimento, poiché la base giuridica del trattamento è in tal caso l'obbligo di legge di cui all'art. 6, lett. c) del GDPR.

Il Titolare, infatti, **non può opporsi** alla richiesta della polizia giudiziaria, la quale, ai sensi dell'art. 354 cpp, potrà procedere al sequestro o intimare al Titolare di conservare le immagini fino a nuova disposizione dell'Autorità.

PRIMO IMPORTANTE ASPETTO DA VALUTARE

1) Per quanto riguarda la **consegna a terzi del filmato** acquisito dalle telecamere, è importante nella fase di valutazione individuare correttamente la terza parte alla quale viene consegnato il filmato, dato che la trasmissione in Paesi extra UE o organizzazioni internazionali è soggetta alle prescrizioni degli articoli 45 e 46 del GDPR (accordi internazionali, decisione di adeguatezza, norme d'impresa vincolanti, ecc.). IN QUESTO CASO IL DESTINATARIO DELLE IMMAGINI È RESIDENTE IN ITALIA.

SECONDO ASPETTO: INFORMAZIONI "COLLATERALI"

Un altro ambito, rispetto al quale il trattamento dei dati acquisiti dalle telecamere di sorveglianza può apparire delicato da valutare, è quello delle informazioni che, indirettamente, si possono trarre dalla grande quantità di immagini che inevitabilmente ogni sistema registra, e che possono rientrare nella categoria dei dati particolari di cui all'art. 9 del GDPR (c.d. sati sensibili).

Si può considerare, per esempio, la ripresa di un soggetto in carrozzina o che porta gli occhiali, che potrebbe far pensare a un trattamento di dati particolari ma che, in realtà, **non è soggetto a riservatezza accentuata**, trattandosi di elementi evidenti, che sono comunque esposti al pubblico. Diversa è la situazione in cui le telecamere riprendono un gruppo di persone che sta parlando di politica o le condizioni di un paziente sottoposto a monitoraggio per motivi di salute. Entrambe le ipotesi rientrano nell'art. 9 del GDPR.

In generale, nell'installare un sistema di videosorveglianza, si dovrebbe sempre procedere a una valutazione dell'ambiente e della possibilità di riprendere anche accidentalmente dati di natura particolare, in base al principio di minimizzazione del trattamento (Data Protection by Default**).Non si dovrebbe riprendere l'ingresso di una chiesa o della sede di un partito politico se non è indispensabile per perseguire la finalità che sta alla base dell'installazione dell'impianto e si dovrebbe comunque valutare la possibilità di mascherare digitalmente l'area che permette di identificare chi entra e chi esce da tali strutture.*

Occorre poi valutare la finalità del trattamento rispetto ai diritti dell'interessato, che potrebbero addirittura giustificare le riprese.

ESEMPIO
Come avviene, per esempio, in ambito sanitario, nel momento in cui è necessario un continuo monitoraggio del paziente per tutelarne la salute e la stessa esistenza in vita e il trattamento rientra pertanto a pieno titolo nella condizione di liceità di cui all'art. 9, co. 2, lett. c) del GDPR.

TERZO ASPETTO IL PRINCIPIO DI ADEGUATEZZA, MISURE DA ADOTTARE

L'adozione di un sistema di rilevazione biometrica comporta, ovviamente, anche il rispetto della condizione di adeguatezza delle **misure di sicurezza** adottate e del **principio di minimizzazione dei dati**. I Titolari del trattamento devono garantire che i dati estratti da un'immagine digitale **non siano eccessivi e contengano SOLO LE INFORMAZIONI NECESSARIE a perseguire la finalità dichiarata**, evitando ogni ulteriore elaborazione.

Tra le misure di sicurezza **dovrebbe essere garantita** la cifratura dei dati o una misura altrettanto efficace per evitare che la diffusione accidentale o la sottrazione dolosa degli stessi possa incidere sui diritti e le libertà degli interessati.

L'EDPB, nelle Linee guida 03/2019, suggerisce l'adozione delle seguenti misure di sicurezza:

- compartimentare i dati durante la trasmissione e l'archiviazione;
- archiviare modelli biometrici e dati grezzi o dati di identità su database distinti;
- crittografare i dati biometrici, in particolare i modelli biometrici, e definire una politica per la crittografia e la gestione delle chiavi;
- integrare una misura organizzativa e tecnica per il rilevamento delle frodi;
- associare un codice di integrità ai dati;
- vietare qualsiasi accesso esterno ai dati biometrici.

CONCLUSIONE

In conclusione è possibile evadere positivamente la richiesta, richiedendo qualora necessarie ulteriori informazioni al richiedente, e avendo cura di analizzare le immagini rilasciate oscurando altri dati/immagini che non "servono" per la finalità del richiedente.

- Inoltre, **va aggiornato il Registro degli accessi**, redatto dal precedente DPO (che trasmetto in allegato), inoltre andrebbe utilizzato la specifica modulistica per le richieste di esercizio dei diritti (in allegato si trasmette il modello redatto dal precedente DPO per l'esercizio dei diritti del GDPR, inoltre si trasmette un nuovo modello - rev.01 - relativo solo al diritto di accesso). Tali modelli di richiesta dei diritti (quindi non il registro), vanno pubblicati e resi disponibili sul sito web istituzionale (qualora non siano già stati pubblicati).

® La scrivente, rimanendo a completa disposizione per chiarimenti/integrazioni del presente parere, ricorda che mantiene costantemente attivi i canali di comunicazione a disposizione della Committenza, al fine di evadere quesiti, dare riscontro a dubbi e redigere l'eventuale documentazione richiesta e necessaria (Email: info@garanteprivacyitalia.it – p.nicolazzo@garanteprivacyitalia.it – PEC: info@pec.garanteprivacyitalia.it – Telefono: 0968.462702 – Mobile: 320.9585082 – FAX: 0968.464273).

11/08/2020

per Multibusiness Srl

GARANTE PRIVACY ITALIA.it
MULTIBUSINESS

Data Protection Officer
Dott. Pasquale Nicolazzo