Comitato europeo per la protezione dei dati: Linee Guida 3/2019 sulla videosorveglianza

19 Febbraio 2020

Terminato il periodo di consultazione pubblica della bozza emanata nel luglio 2019, il Comitato Europeo per la Protezione dei Dati (edpb) ha adottato il 29 gennaio 2020 **la versione definitiva delle Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video** che chiariscono in quali termini il Regolamento 2016/679 si applichi al trattamento dei dati personali quando si utilizzano dispositivi video, e mirano a garantire l'applicazione coerente del GDPR in materia.

Le linee guida

Le linee-guida riguardano sia i dispositivi video tradizionali sia i dispositivi video intelligenti. Per quanto concerne questi ultimi, le linee-guida si concentrano sulle norme relative al trattamento di categorie particolari di dati. Altre tematiche affrontate nel documento riguardano, tra l'altro, la liceità del trattamento, l'applicabilità dei criteri di esclusione relativi ai trattamenti in ambito domestico e la divulgazione di filmati a terzi.

Uso intensivo della videosorveglianza ed impatto sui cittadini

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

Videosorveglianza ed uso improprio

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

Sistemi di videosorveglianza e mglioramento della sicurezza

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

Rischi legati al malfunzionamento

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

Gli algoritmi si baserebbero su dati demografici diversi, quindi, la parzialità nel riconoscimento facciale minaccia di rafforzare i pregiudizi della società. Per questo motivo, i responsabili del trattamento devono anche assicurare che il trattamento dei dati biometrici derivanti dalla videosorveglianza sia sottoposto a una valutazione periodica della sua rilevanza e dell'adeguatezza delle garanzie fornite.

Videosorgeglianza non è di default una necessità

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

Indicazioni sull'applicazione del GDPR

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

Linee_guida_trattamento_dati_personali