www.aipsi.org
AIPSI - ISSA Italian Chapter
www.issa.org

6/7/2021 ore 18-20

Webinar AIPSI-CSIG Parte 1° "Intelligenza Artificiale, GDPR e Videocontrollo: la nuova bozza del regolamento europeo e l'impatto per le organizzazioni"

AIPSI ed il Centro Studi di Informatica Giuridica di Ivrea Torino (CSIG) organizzano due webinar, interdisciplinari e tra loro sequenziali e correlati, sul tema della videosorveglianza. La nuova normativa europea ed italiana sul tema e l'introduzione di tecniche di Intelligenza Artificiali stanno modificando in maniera significativa le modalità d'uso e di gestione dei sistemi di video sorveglianza. Il 2° webinar si terrà il 13/7/2021 allo stesso orario e tratterà "La gestione del Videocontrollo nelle organizzazioni : le nuove sanzioni, ispezioni e audit".
Con questi due seminari AIPSI- CSIG intendono approfondire l'attualissimo tema, facendo anche riferimento alla recente pubblicazione del libro "Video sorveglianza e GDPR" a cura di Mauro Alovisio, edizioni Giuffrè, 2021 (https://shop.giuffre.it/024211142-videosorveglianza-e-gdpr.html)

L'agenda dei lavori di questo webinar prevede:

- *Apertura del webinar* - Marco R. A. Bozzetti, Presidente AIPSI e CEO Malabo Srl
- *I Sistemi di videocontrollo: le novità delle linee guida del Comitato europeo per la protezione dei dati personali* - Mauro Alovisio, coordinatore del corso di perfezionamento universitario in materia di GDPR dell'Università degli Studi di Torino e docente a contratto presso Università Statale di Milano
- *Videocontrollo, Intelligenza artificiale e riconoscimento facciale* - Alessandro del Ninno, Avvocato e professore universitario - esercita a Roma come Of Counsel dello Studio legale Tonucci & Partners
- *I sistemi di videosorveglianza integrata nelle città* - Stefano Manzelli, consulente e coordinatore della sicurezza urbana in fase di progettazione strategica, direttore del Portale www.sicurezzaurbanaintegrata.it.

Sistemi di videocontrollo: le novità delle linee guida del Comitato europeo per la protezione dei dati personali –

6 luglio 2021

avv. Mauro Alovisio

Ciao !

Mauro Alovisio

Avvocato presso Avvocatura e Servizi legali

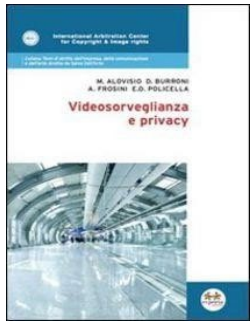
Coordinatore del corso di perfezionamento in materia di protezione dei dati personali Università di Torino (prof. Pizzetti e prof. Foà)

Professore a contratto presso Università Statale di Milano

Direttore del Centro Studi di Informatica Giuridica di Ivrea Torino

Fellow del centro di ricerca Nexa del Politecnico di Torino

Socio Associazione Italiana Formatori



Centro Studi di Informatica Giuridica di Ivrea Torino

Il Centro Studi di Informatica Giuridica di Ivrea-Torino (CSIG) è un' associazione indipendente senza finalità di lucro attiva dal 2005 interdisciplinare (rivolta a giuristi, informatici, etc.)

Mission: aggiornamento professionale, studio, approfondimento dell'evoluzione dei diritti digitali, dell'ICT e dell'Informatica Giuridica a livello locale e nazionale

Aderisce alla rete nazionale alla relativa mailing list (900 professionisti)

A livello piemontese: ha due sedi una storica a Ivrea e una a Torino, un blog http://csigivreatorino.it ed un Comitato Scientifico di magistrati, professori e avvocati.

Ha partecipato alle consultazioni on line in materia di droni, trasparenza, open data. software libero, wi-fi, cyberbullismo, etc..

Prossime azioni

La tutela della vita digitale del minore

A cura di Fabio Di Resta
Prefazione di Franco Pizzetti

ITER

22 settembre 2021 – ICT day Intelligenza artificiale – Club Dirigenti di Informatica

10 ottobre 2021 , presentazione libro AA:VV: «La tutela della vita digitale del minore» edizione Iter

22 Ottobre 2021 , convegno nazionale in materia di telemedicina 2021

Agenda

Perché occuparsi di videocontrollo?

Qual è il legame fra videocontrollo e protezione dei dati

Quali sono gli impatti delle nuove linee guida in materia di videosorveglianza?

Le ragioni dello sviluppo del videocontrollo

- Tecnologia diffusa ed in evoluzione

- Aumento degli incentivi economici (finanziamenti europei, nazionali e regionali connessi alla sicurezza)

-Ambito di applicazione molto ampio finalità molteplici: sicurezza pubblica, organizzative, produttive, di sicurezza sul lavoro o di tutela del patrimonio aziendale

-Aumento delle segnalazioni, degli esposti e delle ispezioni al Garante per la protezione dei dati personali e della Guardia di Finanza

Questo volume, tutto dedicato a aiutare il lettore a comprendere meglio le mille sfaccettature che presentano oggi i sistemi di videosorveglianza e le mille, e spesso differenti, regolazioni che ne disciplinano l'uso a seconda dei contesti in cui la videosorveglianza è adottata e delle finalità perseguite, presenta molti pregi che ne raccomandano la lettura tanto a chi sia già al corrente, anche per ragioni professionali, di questa tematica, quanto per chi invece ad essa si voglia avvicinare.

Il primo e il più importante pregio è il linguaggio e il metodo di esposizione adottato in tutti i saggi semplice ma tecnico che consente al lettore di seguire un filo logico.

Il secondo pregio del volume è che tutti i saggi forniscono al lettore una documentazione ampia e accurata sulle norme a tutela della privacy e delle persone.

In soccorso tutti gli Autori, a cominciare Mauro Alovisio, prendono per mano il lettore, sia esso uno specialista o un cittadino interessato a capire queste nuove tecnologie, e lo accompagnano mano nella mano a capire sempre meglio i temi che il loro uso solleva e i rischi, ma anche le grandi opportunità, che questi sistemi, se ben usati da persone davvero competenti, possono offrire a tutti, sia aumentando la sicurezza delle persone sia mettendo a disposizione di tutti, soprattutto nell'ambito urbano (le famose smart cities) nuove possibilità di utilizzo dei mezzi di trasporto e della regolazione del traffico. Migliorando così la vita di tutti e dilatando le potenzialità delle relazioni sociali nella Digital Age.

Prezioso, in questo senso, è il saggio di Stefano Manzelli che aiuta a capire le grandi opportunità di queste tecnologie se correttamente applicate anche ai sistemi sociali e alle relazioni che ne costituiscono l'ossatura.

Infine un ulteriore e importantissimo pregio del volume consiste nel non occuparsi solo degli aspetti tecnici e organizzativi della videosorveglianza ma di dedicare attenzione specifica anche alla necessità di adeguare i moduli organizzativi interni delle strutture che ne fanno uso, al fine non solo di massimizzare le opportunità ma anche le tutele e le garanzie per tutti. Il saggio di Colatina, insieme a quelli di Nicola di Mare e Alessandro Del Ninno, che si occupa specificamente della tematica applicata ai luoghi di lavoro, aiutano i lettori a capire quanto dinamica sia la Digital Age e di conseguenza quanto flessibile e costantemente attento all'innovazione debba essere l'uso delle nuove tecnologie quando esse presentino, insieme a grandi opportunità, anche rischi oggettivi per le persone e la convivenza sociale.

Il saggio di Luca Trevisoli sulle sanzioni relative a un cattivo uso delle tecniche di videosorveglianza consente infatti anche al lettore meno esperto di capire bene quanto nei confronti di queste nuove tecnologie sia importante l'attività di controllo e di sanzione.

Il volume costituisce uno strumento utile e prezioso, anche per gli operatori tecnici e giuridici del settore. Esso infatti aiuta chiunque debba misurarsi con la videosorveglianza per ragioni professionali, sia esso un legale o un tecnico, a avere davanti un panorama informativo di altro valore anche tecnico ed estremamente informato e aggiornato.

di Franco Pizzetti

MAURO ALOVISIO
Avvocato presso Università, si occupa da diversi anni di protezione dati e del diritto delle nuove tecnologie, è coordinatore del corso di perfezionamento universitario in materia di protezione dei dati personali del Dipartimento di Giurisprudenza dell'Università degli Studi di Torino, professore a contratto presso l' Università Statale di Milano, presidente del Centro Studi di informatica Giuridica di Ivrea Torino, Fellow del Centro di ricerca Nexa su Internet e società del Politecnico di Torino; autore di pubblicazioni ed articoli in materia di protezione dati personali, videosorveglianza, formatore e relatore a convegni e seminari.

Compliance

PRIVACY

VIDEOSORVEGLIANZA E GDPR

Profili di *compliance* nelle imprese e nelle pubbliche amministrazioni

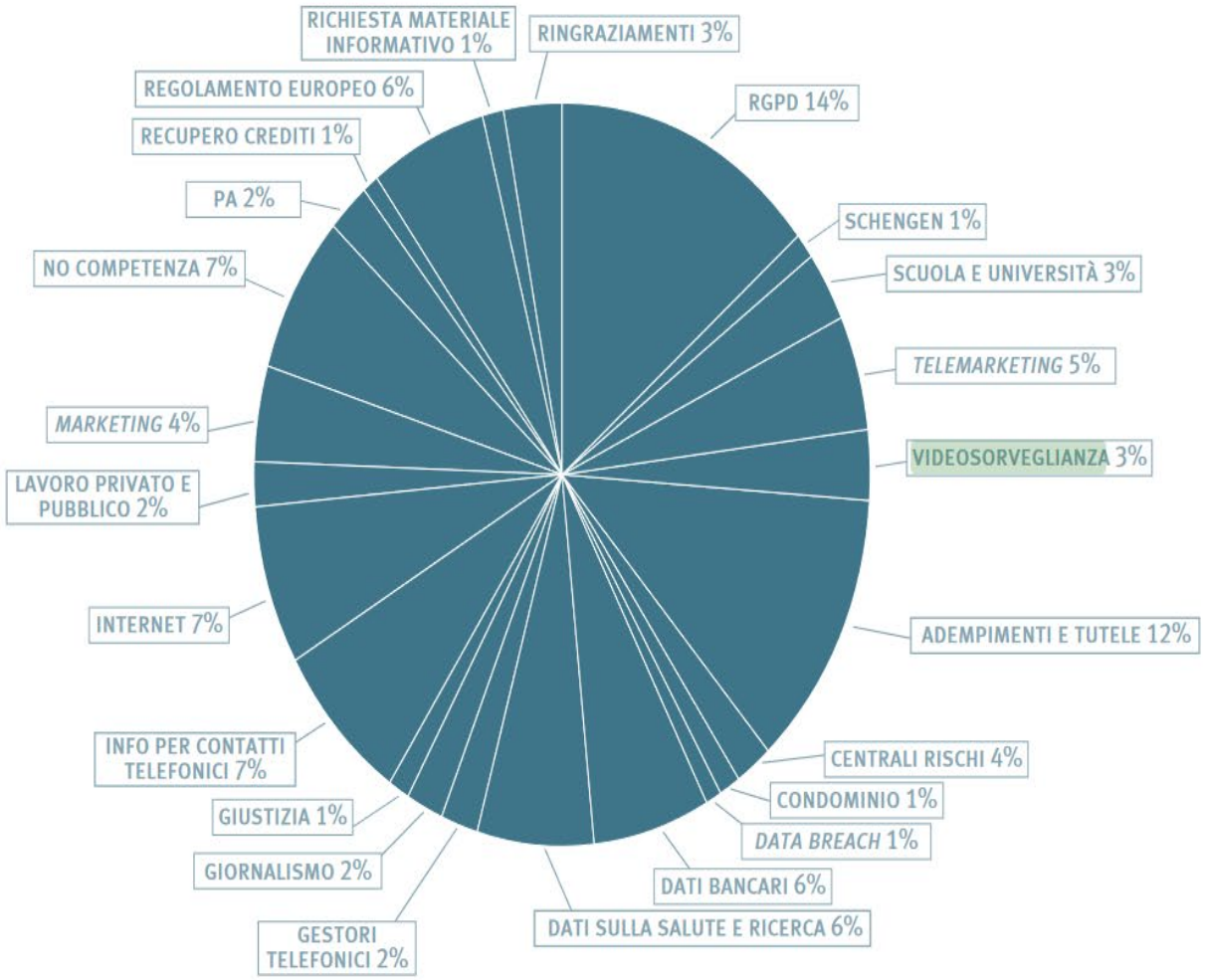
a cura di Mauro Alovisio

ISBN 078-88-28-83174-7

€ 00,00
02421142

GIUFFRÈ FRANCIS LEFEBVRE

Grafico 16. Oggetto delle *e-mail* esaminate dall'Urp



luogo quelle concernenti gli adempimenti introdotti dal RGPD (circa 2.160 *e-mail* ricevute, delle quali circa 1.500 hanno riguardato la designazione del Responsabile della protezione dei dati e la procedura *online* realizzata dal Garante per la comunicazione dei dati di contatto dello stesso).

Altre questioni oggetto di interesse hanno riguardato i trattamenti di dati personali per finalità di *direct marketing* (oltre 950 *e-mail*) e, in particolare, di *telemarketing* (530 *e-mail*); la videosorveglianza in ambito privato, lavorativo e scolastico (oltre 340 *e-mail*); l'accesso ai dati bancari (oltre 620 *e-mail*) e la tutela degli interessati in relazione ai trattamenti effettuati dai sistemi di informazione creditizia (192 *e-mail*); ulteriori ambiti di interesse sono rappresentati dai trattamenti di dati personali effettuati in internet, nei *social network*, tramite le *app*, nonché in ambito giornalistico, con particolare riferimento alle richieste di deindicizzazione dei dati personali dai motori di ricerca volte all'esercizio del cd. diritto all'oblio di cui all'art. 17 del RGPD (in totale 928 *e-mail*).

Il maggior numero delle richieste pervenute ha riguardato la tutela dei dati personali nei diversi ambiti economico-sociali interessati dalle misure previste dai decreti adottati al fine di contrastare l'emergenza da Covid-19. In tale contesto si segnalano, in particolare, le istanze relative al rispetto della normativa in materia di protezione dei dati personali con riferimento alla attribuzione dei contributi economici (in particolare, dei cd. buoni spesa) da parte dei comuni ai soggetti in condizioni di disagio economico.

L'Urp si è occupato del tema dell'erogazione da parte dell'Inps dei cd. *bonus* Covid a sostegno del reddito, questione esaminata dal Garante con riguardo alle violazioni dei dati personali verificatesi in occasione dell'avvio delle procedure per

Videosorveglianza illegittima, per il risarcimento del danno occorre dimostrare un pregiudizio effettivo

Speciali Venerdì, 25 Giugno 2021 07:11

Ai fini del risarcimento del danno non patrimoniale per violazione del diritto alla riservatezza, è necessario che l'offesa sia grave, ossia che il diritto sia inciso oltre

NOTE AUTORE

Federprivacy
Federprivacy è la principale associazione di riferimento in Italia dei professionisti della privacy e della protezione dei dati personali, iscritta presso il Ministero dello Sviluppo Economico ai sensi della Legge 4/2013. Email: **urp@federprivacy.org**

NEWS FOCUS PIÙ LETTI

Diritto all'Oblio: se il
venti anni prima non
giornalistico, ok alla
nell'archivio online e
cartaceo
Martedì, 29 Giugno 2021 07:13

Green pass, gli addett
devono avere un'incar
essere istruiti
Lunedì, 28 Giugno 2

Trasferimenti di dati
extra UE: le nuove Cla
Contrattuali Standard
Venerdì, 25 Giugno

Videosorveglianza ille
risarcimento del dann
dimostrare un pregiu
Venerdì, 25 Giugno

Oltre 150.000 videocamere di sicurezza hackerate, anche Tesla tra le vittime

10 Marzo 2021 21

Un sistema di videosorveglianza basato su una piattaforma cloud ha molteplici vantaggi - tra cui l'accesso da remoto - ma anche diverse debolezze. Se un malintenzionato riesce a trovare una falla nel sistema può prendere il controllo di un'articolata rete di videocamere e il caso che ha recentemente riguardato **Verkada** lo dimostra in modo eloquente. Un gruppo di hacker è riuscito a **violare la piattaforma di videocamere di sicurezza della startup e ad accedere ai**

BIOMETRIA E PRIVACY

Il caso svedese. Riconoscimento facciale e dati biometrici, cosa dice il GDPR?

di **Nicola Fabiano, Studio Legale Fabiano** | 2 Settembre 2019, ore 15:30

Una società di riconoscimento facciale dovrà cancellare i dati di un cittadino europeo

di **Raffaele Angius**
Contributor
3 FEB, 2021

Il Garante della privacy della città di Amburgo ha accolto il ricorso di un cittadino contro la società statunitense Clearview, ma è una vittoria a metà

Riconoscimento facciale (Getty Images)

Riconoscimento facciale, Garante boccia sistema Viminale

"Si rischia una forma di sorveglianza indiscriminata di massa"

Redazione ANSA
ROMA

16 aprile 2021
17:45
NEWS

Riconoscimento facciale, Garante boccia sistema Viminale - CLICCA PER

AMMINISTRATIVO

PRIVACY | 09 Febbraio 2021

Il Garante Privacy pubblica il piano di ispezioni del primo semestre 2021

di Mauro Alovisio - Avvocato

Il Garante per la protezione dei dati personali illustra, nell'ottica di informazione e comunicazione istituzionale, nel programma ispettivo le aree di intervento definite nel primo semestre 2021: le violazioni della sicurezza dei dati (data breach); i trattamenti di dati effettuati da "data broker"; il riconoscimento facciale mediante sistema di videosorveglianza.

-A A+

Il Garante per la protezione dei dati personali definisce, attraverso la deliberazione del 10 dicembre 2020, il **programma delle ispezioni di ufficio** pianificate nel primo semestre 2021 ed individua molteplici specifiche aree di intervento.

Il Garante definisce, attraverso il piano, le priorità in relazione alle risorse disponibili, e individua principi e criteri dell'attività ispettiva.

L'attività ispettiva di iniziativa del Garante ricomprende l'**accertamento in loco** curato dal personale dell'Ufficio o delegato alla Guardia di Finanza nei luoghi dove si effettuano i trattamenti di dati, o nei quali occorre effettuare rilevazioni comunque utili al medesimo controllo, nei confronti di soggetti non necessariamente individuati sulla base di reclami o segnalazioni.

La sopra citata delibera illustra gli ambiti del controllo e gli obiettivi numerici da conseguire.
Il provvedimento in esame tiene conto dei procedimenti ispettivi e sanzionatori in corso nonché di quelli avviati sulla base della precedente programmazione e non

Notizie correlate

Il TAR Lazio dà ragione agli estetisti: centri aperti in zona rossa, come i parrucchieri

Pratiche commerciali scorrette: Sky sanzionato dall'Antitrust

COVID-19: prosegue il divieto di spostamento tra le Regioni

Il furto dell'hard disk esterno costa caro all'agenzia regionale per l'ambiente

Il Garante su data breach sanitari, uso delle impronte digitali dei dipendenti e riconoscimento facciale

Piano ispettivo 2021

Le ispezioni riguarderanno sia il **settore pubblico** che il **settore privato**.

L'attività di ispezione del Garante sarà focalizzata sui seguenti profili:
- accertamenti in riferimento a profili di interesse generale nell'ambito di **trattamenti di dati biometrici** per il riconoscimento facciale anche mediante sistemi di videosorveglianza;
- trattamenti di dati personali nel settore della c.d. "**videosorveglianza domestica**" e nel settore dei sistemi audio/video applicati ai giochi (c.d. **giocattoli connessi**);
- trattamenti di dati personali effettuati da "**data broker**";
- trattamenti di dati personali effettuati da società rientranti nel settore denominato "**Food Delivery**";
- **data breach**.

13.3. *I trattamenti di dati personali effettuati mediante sistemi di videosorveglianza*

Il Garante ha continuato ad occuparsi del trattamento dei dati effettuato attraverso sistemi di videosorveglianza installati presso luoghi di lavoro, rammentando ai titolari del trattamento l'obbligo di rispettare l'art. 114 del Codice (che rinvia all'art. 4, l. n. 300/1970), l'obbligo di fornire un'adeguata informativa agli interessati prima che entrino nel campo di ripresa delle telecamere nonché la necessità di effettuare il trattamento solo in presenza di una specifica condizione di liceità del trattamento.

Videosorveglianza in assenza di informativa

Sempre con riferimento ad un trattamento di dati personali effettuato attraverso un sistema di videosorveglianza, a seguito di una segnalazione, il Garante, dopo avere delegato al Nucleo speciale tutela *privacy* e frodi tecnologiche l'accertamento ispettivo presso la sede legale del titolare del trattamento, ha adottato un'ordinanza-ingiunzione nei confronti di una struttura ricettiva, avendo accertato che la stessa, a partire dal 2009 (e fino alla data dell'accertamento ispettivo), aveva utilizzato un impianto di videosorveglianza all'interno e all'esterno della struttura omettendo di apporre, in prossimità del raggio di azione delle telecamere, cartelli informativi idonei ad avvisare clienti, dipendenti e fornitori della esistenza e delle caratteristiche essenziali dell'attività di videoripresa, in contrasto con quanto stabilito dall'art. 13 del RGPD (provv. 26 novembre 2020, n. 256, doc. web n. 9533587).

Videosorveglianza non conforme all'autorizzazione

A seguito della presentazione di tre reclami aventi per oggetto i medesimi fatti, è stata irrogata una sanzione pecuniaria nei confronti di una società con la quale i reclamanti avevano stipulato un contratto di *catering* e *banqueting*. L'Autorità, a seguito dell'accertamento ispettivo presso la sede legale della società delegato al Nucleo speciale tutela *privacy* e frodi tecnologiche, ha accertato che il titolare del trattamento aveva fatto installare e utilizzato un impianto di videosorveglianza con caratteristiche non conformi a quanto prescritto nell'autorizzazione rilasciata dall'Ispettorato

29 ottobre 2020, n. 213, doc. web n. 9518849).

Ha altresì formato oggetto di vaglio l'installazione, avvenuta ad opera di un'azienda sanitaria, di un sistema di videosorveglianza dotato di telecamere dislocate in aree nelle quali normalmente transitano o sostano anche i dipendenti (corridoi, ingressi, sale di attesa, pronto soccorso), con conseguente possibilità di controllarne indirettamente l'attività. Nel corso dell'istruttoria è emerso che l'installazione dei citati sistemi – avvenuta da oltre dieci anni in diverse strutture di competenza dell'azienda sanitaria e funzionale a esigenze di sicurezza e di tutela del patrimonio aziendale – fosse stata effettuata in assenza del necessario previo accordo con le organizzazioni sindacali o dell'autorizzazione da parte del competente Ispettorato del lavoro.

Videosorveglianza in assenza di autorizzazione

In base alla disciplina in materia di protezione dei dati personali, l'amministrazione, che opera in qualità di datore di lavoro, può trattare i dati personali dei dipendenti se il trattamento è necessario per la gestione del rapporto di lavoro e per adempiere a specifici obblighi o compiti previsti dalla normativa nazionale o dell'Unione (artt. 6, par. 1, lett. *c*); 9, par. 2, lett. *b*) e 4; 88 del RGPD) rispettando altresì le norme nazionali, preesistenti o di futura emanazione, che "includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati in particolare per quanto riguarda la trasparenza del trattamento […] e i sistemi di monitoraggio sul posto di lavoro" (cons. 155, artt. 6, par. 2 e 88, par. 2, del RGPD). Sul punto, il Codice, confermando l'impianto anteriore alle modifiche apportate dal d.lgs. 10 agosto 2018, n. 101, fa espresso rinvio alle disposizioni nazionali di settore che tutelano la dignità delle persone sul luogo di lavoro, con particolare riferimento ai possibili controlli a distanza da parte del datore di lavoro (artt. 113 e 114 del RGPD).

In merito, nel solco di precedenti decisioni, l'Autorità ha ulteriormente chiarito che le esigenze di sicurezza e di tutela del patrimonio, pure invocate nel caso di specie dall'azienda, non sono per sé sole sufficienti a legittimare la presenza di tali dispo-

DALL'AUTORITA' PER LA PROTEZIONE DEI DATI DELLA SVEZIA: Le body cam di SL sono contro la legge

22/06/2021 Autorità di controllo, Svezia

This post is also available in: English, Español, Français

L'autorità per la protezione della privacy IMY, emette una tassa di sanzione amministrativa nei confronti di SL di 16 milioni di corone svedesi (1.572.192,00 euro).
SL ha violato l'ordinanza sulla protezione dei dati quando i controllori dei biglietti sono dotati di body cam che registrano immagini e suoni.
L'IMY, in precedenza l'Ispettorato dei dati svedese, ha esaminato l'uso da parte di SL di body cam, SL ha dotato i controllori di biglietti di telecamere indossabili. Lo scopo delle telecamere è prevenire situazioni minacciose, documentare incidenti che si sono verificati e garantire che la persona giusta venga multata per aver viaggiato nel traffico locale di Stoccolma senza una patente di guida valida.

Search

Cerca

Recent Posts

DALL'AUTORITA' PER LA PROTEZIONE DEI DATI DELLA GERMANIA: Adozione delle decisioni di adeguatezza del Regno Unito

DALL'AUTORITA' PER LA PROTEZIONE DEI DATI DELLA FINLANDIA: La Commissione Europea ha preso due decisioni sull'adeguatezza della protezione dei dati britannica

DALL'AUTORITA' PER LA PROTEZIONE DEI DATI DELLA POLONIA: Il numero di registro fondiario e ipotecario consente di identificare facilmente il proprietario dell'immobile

DALL'AUTORITA' PER LA PROTEZIONE DEI DATI DELLA NORVEGIA: La Commissione Europea con una decisione di adeguatezza per il Regno Unito

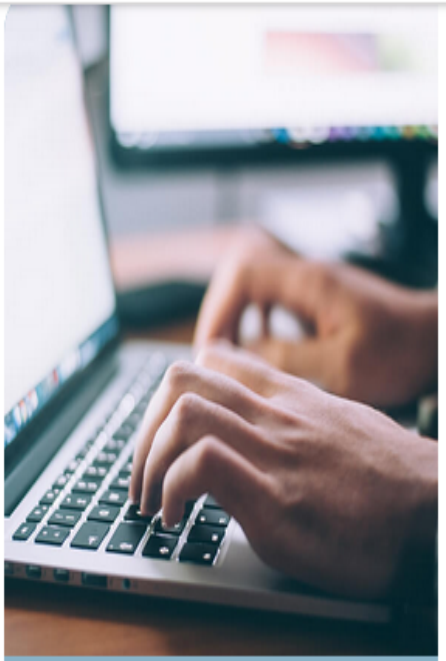
DALL'AUTORITA' PER LA PROTEZIONE DEI DATI DELLA FRANCIA: Rifiutare i cookie deve essere semplice come accettare: conformità di tutte le organizzazioni

Sanzioni | 14.1.2021 | *Federprivacy*

Videosorveglianza dipendenti: DPA Bassa Sassonia infligge multa di 10,4 milioni di euro

Videosorveglianza indiscriminata sui dipendenti negli ambienti di lavoro, maxi multa da 10 milioni di euro per l'azienda

Il DPA della Bassa Sassonia ha inflitto una multa di 10,4 milioni di euro al rivenditore di elettronica notebooksbilliger.de, che ha monitorato attraverso un sistema di videosorveglianza i suoi dipendenti per almeno due anni senza avere una base giuridica per farlo. Tra le aree coperte dalle telecamere anche i luoghi di lavoro, le aree di vendita, i magazzini e le aree ricreative. La società ha dichiarato che lo scopo delle videocamere installate era prevenire e indagare su atti criminali e monitorare il movimento delle merci nei magazzini. Tuttavia, per prevenire il furto, un'azienda deve prima considerare metodi più blandi. Inoltre, la videosorveglianza per rilevare atti criminali è consentita solo se esiste un ragionevole sospetto nei confronti di persone specifiche. In tal caso, potrebbe essere consentito monitorarli con telecamere per un periodo di tempo limitato. Su notebooksbilliger.de, tuttavia, la videosorveglianza non era limitata a un periodo specifico né a dipendenti specifici. Inoltre, in molti casi le registrazioni venivano archiviate per 60 giorni, un tempo significativamente più lungo del necessario. Anche i clienti di notebooksbilliger.de sono stati colpiti dalla videosorveglianza illegale, poiché alcune telecamere sono state puntate verso le aree salotto nell'area di vendita. Finora, la multa contro notebooksbilliger.de è la sanzione più alta che il DPA della Bassa Sassonia ha emesso ai sensi del GDPR.



Eventi

Sanzioni

-La violazione dei principi sul trattamento dei dati indicati dall' art. 5 GDPR comporta l'applicabilità delle sanzioni di cui all'articolo 83, comma 5 del GDPR (fino a **20.000.000 EUR,** o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore).

nel caso di comunicazione o diffusione delle immagini a terzi destinatari ubicati al di fuori della UE in violazione delle prescrizioni di cui agli articoli da 44 a 49 del GDPR sanzioni **fino a 20.000.000** EUR, o per le imprese, fino al 4% del fatturato mondiale

-violazione de gli obblighi in materia di DPIA e di nomina del RPD nel caso di videosorveglianza su larga scala (v. articoli 35 e 37 GDPR) sanzione prevista dall'articolo 83, comma 4 del GDPR (fino a 10.000.000 EUR, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore

VIDEOSORVEGLIANZA

Torino e telecamere intelligenti, l'altolà del Garante al Comune

Sotto la lente del Garante della Privacy è finito Argo, l'annunciato impianto di videosorveglianza intelligente promesso dalla giunta Appendino

di Paolo Coccorese

LAVORO

PRIVACY | 26 Maggio 2021

Controllo a distanza dei lavoratori: senza accordi sindacali o il via libera dell'ispettorato meglio togliere le telecamere

di Stefano Manzelli

Non è opportuno presentare all'Ispettorato del lavoro richieste finalizzate alla regolarizzazione tardiva degli impianti di videosorveglianza interferenti con la tutela dei lavoratori. Perché se dalla domanda emerge che si tratta di un tentativo di sanatoria scatterà l'ispezione con possibili conseguenze penali.

-A A+

Lo ha chiarito l'Ispettorato nazionale del lavoro con la nota n. 797 del 18 maggio 2021. I confini normativi della videosorveglianza nell'ambito dei luoghi di lavoro sono dettati dallo statuto dei lavoratori dove si prevede...

Qui la nota dell'INL del 18 maggio 2021, n. 797

Notizie correlate

Identità, preesistenza ed autonomia: le tre grazie del trasferimento d'azienda

Avvocati: alla Corte Costituzionale la questione sull'iscrizione alla gestione separata

Assegno temporaneo per figli minori, al via le domande dal 1° luglio

Totalizzazione: la pensione si calcola con il metodo retributivo o con quello contributivo?

Legittima la sanzione per il lavoratore in caso di mancato utilizzo della mascherina

I più letti | Oggi | Settimana | Mese

1 Avvocati: alla Corte Costituzionale la questione sull'iscrizione alla gestione

DeG | Accedi

TD
Redazione Bruxelles
22 giugno 2021 15:47

NETWORK

"No al riconoscimento facciale nei luoghi pubblici": l'appello del Garante Ue per la protezione dei dati

La richiesta di un divieto totale arriva dopo la proposta della Commissione, che vuole usare l'intelligenza artificiale per combattere la criminalità

Si parla di
artificiale
intelligenza
privacy
sorveglianza
ue

No al riconoscimento facciale. Gli organismi Ue di vigilanza sulla privacy hanno chiesto un divieto generale di qualsiasi uso delle tecnologie di intelligenza artificiale per

I più letti

1. EUROPA
Bambini morti negli istituti religiosi, sfregiata con 'mani insanguinate' la statua di papa Wojtyla

2. NETWORK
Svolta per le donne ceche, il loro cognome potrà non essere più declinato al femminile

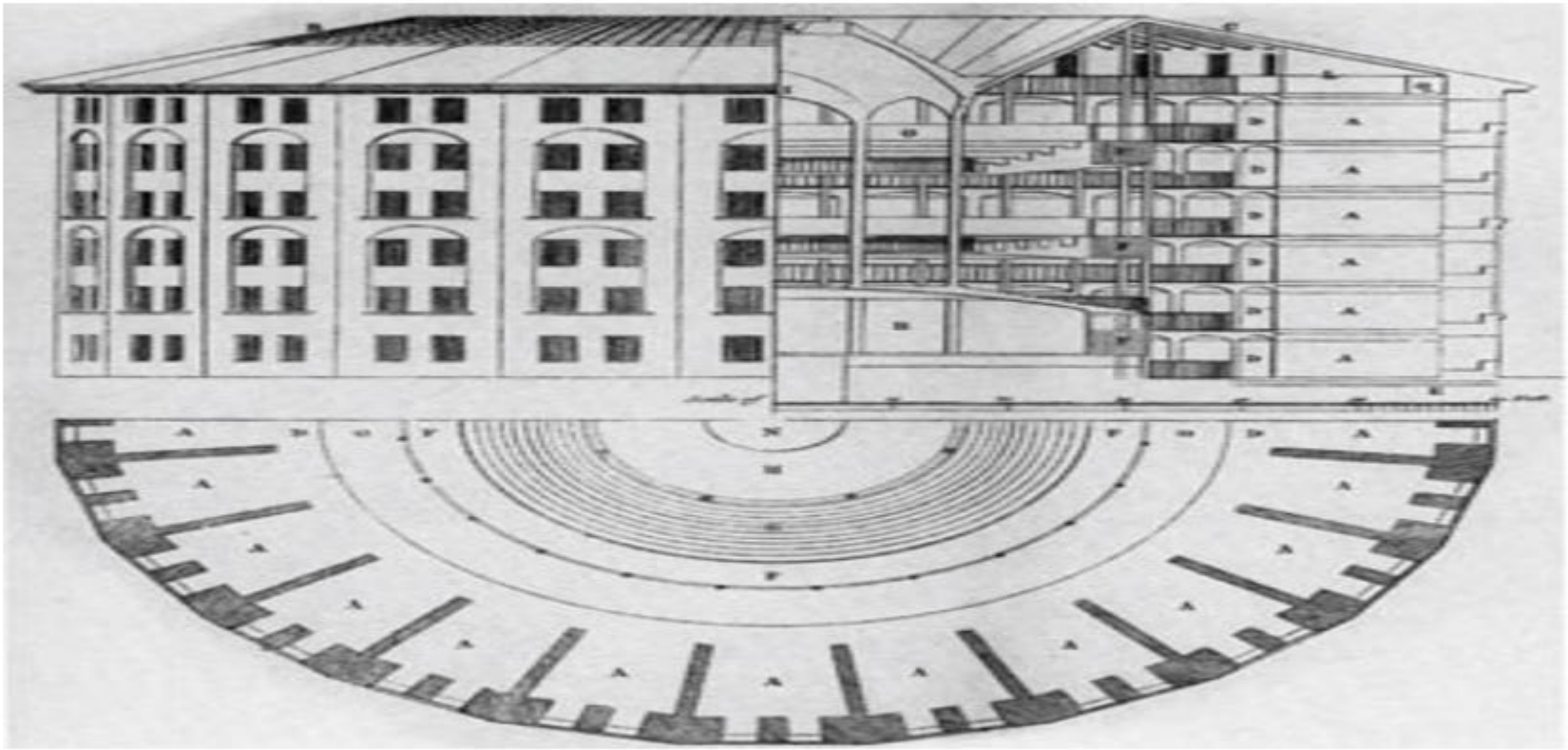
Agenda

Perché occuparsi di videocontrollo?

Qual è il legame fra videocontrollo e protezione dei dati

Quali sono gli impatti delle nuove linee guida in materia di videosorveglianza?

Bentham: Panopticon, 1791



STRATEGIE

Sorveglianza di massa in Cina, il modello che spaventa l'Occidente

Spyware nei cellulari, telecamere per il riconoscimento facciale, wi-fi sniffer. Si basa su un mix di tecnologie vecchie e nuove la grande rete voluta dal presidente Xi Jinping che punta a "spiare" 1,4 mld di abitanti. Il prezzo pagato alla privacy del nuovo Panopticon che spaventa il mondo

04 Mar 2020

Barbara Calderini
Legal Specialist - Data Protection Officer

Rischi della videosorveglianza

- **Dimensione spaziale:**
spazio privato: libertà di non essere disturbati dall'esterno (dimensione passiva)

- **Dimensione informazionale:**
riguarda il flusso delle informazioni personali. il controllo della persona nei confronti del trattamento dei dati personali

- Dimensione decisionale:
libertà della persona di prendere delle decisioni - libertà dell'uomo (Panopticon di Bentham) strumento di libertà e di partecipazione diritto non elitario ma del cittadino digitale

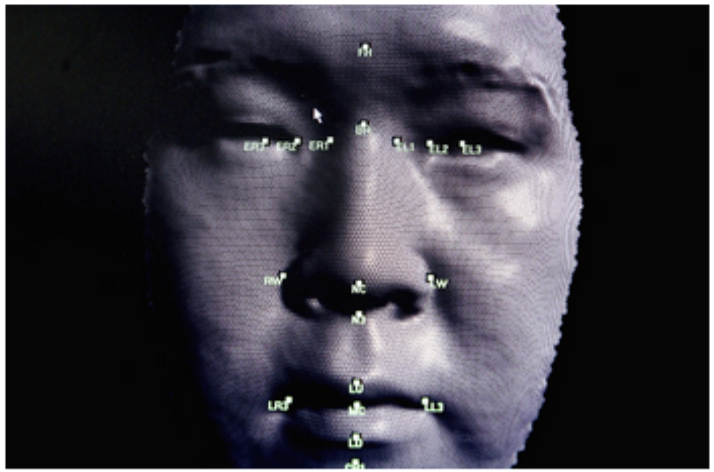
- ***Spazio morale**: rischio di discriminazione , rischio endemico (etnia, genere, colore della pelle, religione, opinioni politiche v. Chiara Fonio, "Videosorveglianza senza volto")*
- ***Creazione di un corpo e di un'identità elettronica diversa dall'identità fisica**: Habeas corpus Magnas Charta del 1215 Habeas data (Rodotà)*

Charlin Chaplin Tempi Moderni , 1938

di **Kevin Carboni**
Contributor
14 APR, 2021

Come è andata a finire la prima causa sul riconoscimento facciale in Cina

Per la prima volta una corte ha sancito il diritto dei cittadini a richiedere la cancellazione dei dati personali raccolti da un privato con strumenti biometrici



(Foto: Ian Waldie/Getty Images)

Immagine, dato personale e videosorveglianza

-Le immagini registrate dagli impianti di videosorveglianza sono qualificabili come “dati personali”, in quanto consentono di identificare, anche indirettamente, singoli individui

(Provv. 8 aprile 2010, doc. web n. 1712680; v. anche, del Gruppo di lavoro dei Garanti europei, parere n. 8/2001 wp 48 e parere 4/2007 sulla nozione di “dato personale”, wp 136

Le operazioni di raccolta e registrazione di immagini e suoni, effettuate con queste apparecchiature, costituiscono un trattamento di dati personali, che deve essere conforme alle disposizioni in materia (cioè GDPR)

Dati biometrici: la definizione GDPR

- ✓l'art. 4, paragrafo 1, n. 14) del GDPR, definisce i dati biometrici come quei "dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne **consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici".**

Definizione di videosorveglianza?

- **non è presente nel nostro ordinamento una definizione di videosorveglianza!!**

- non vi è una legge specifica in materia ma un corpo di norme stratificate:

  - ❑codice penale: divieto di interferenze illecite nella vita privata, tutela del domicilio
  - ❑codice civile: tutela dell'immagine
  - ❑statuto dei Lavoratori (legge 300 del 1970)
  - ❑normative specifiche: sicurezza degli stadi, impianti sportivi, musei, biblioteche etc.
  - ❑Normativa europea (GDPR)
  - ❑D.lgs 196/03 come modificato dal d.lgs 101/18
  - ❑Provvedimenti del Garante
  - ❑Circolari INPS

Bussola giuridica

Il regolamento privacy europeo 679 del 2016

Le linee guida 3 del 2019 del Comitato europeo per la protezione dei dati personali ad oggetto: il trattamento dei dati effettuato mediante apparati video

Provvedimento generale del Garante privacy del 8 aprile 2010

Il precedente provvedimento del Garante privacy del 29 aprile 2004

- Gruppo di lavoro Garanti Europei " (parere 11 febbraio 2004, n. 4)

"attività mirante al controllo a distanza di eventi, situazioni e avvenimenti mediante acquisizione di immagini, eventualmente in associazione con dati sonori e/o biometrici, ad esempio le impronte digitali"

Videosorveglianza e GDPR

Il GDPR approfondisce il profilo del **monitoraggio automatico sistematico** in diversi punti:

-art. 35, paragrafo 3) lett.c c), che prevede come misura di protezione dei dati la valutazione d'impatto **in caso di monitoraggio sistematico di un'area accessibile al pubblico su larga scala,** *«la sorveglianza sistematica su larga scala di una zona accessibile al pubblico»*

-art. 37,paragrafo 1,lettera b), obbligo dei Titolari del trattamento di designare un Responsabile per la Protezione dei dati se il **trattamento per sua natura comporta un monitoraggio regolare e sistematico degli interessati su larga scala (attività principale del titolare**

- art. 88 Trattamenti di dati nell'ambito del rapporto di lavoro : Tali norme includono misure appropriate e specifiche a salvaguardia della dignità u mana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, ….. sistemi di monitoraggio sul posto di lavoro.

Nozione di videosorveglianza nelle linee guida del Comitato dei Garanti Europei

Le linee guida **sottolineano l'assenza di una definizione di videosorveglianza** nel GDPR e richiamano **la regola tecnica EN 62676-1-1:2014** Video surveillance systems for use in security applications – Part 1-1: Video system requirements, che definisce tre elementi fondamentali che costituiscono un sistema di videosorveglianza ("VSS") sono:

1. ambiente video;
2. gestione del sistema;
3. sicurezza del sistema

I componenti di un sistema di videosorveglianza possono essere cosi suddivisi:

1. mezzi di ripresa;
2. mezzi di visualizzazione;
3. mezzi di videoregistrazione;
4. mezzi di trasmissione.

I principi del GDPR devono essere incorporati in ciascuno dei componenti e applicati durante tutto il ciclo di vita

Visione delle linee guida (a)

La videosorveglianza ha implicazioni massive sul trattamento dei dati personali
(rischi di utilizzo improprio dei dati e di usi secondari dei trattamenti, tecniche altamente performanti v. IA, algoritmi, rischi di pregiudizi e discriminazioni)

La videosorveglianza non è di default una necessità quando esistono altri mezzi per raggiungere la finalità : N.B.pertanto la videosorveglianza è da adottare solo quando non è possibile raggiungere lo stesso scopo con modalità meno intrusive.

Altrimenti, secondo il Comitato dei Garante Europei si rischierebbe un cambiamento nelle norme culturali che porta come principio generale all'accettazione della mancanza della privacy

Visione delle linee guida b)

Le linee guida del Comitato Europeo dei Garanti europei hanno la finalità **di promuovere l'applicazione coerente del regolamento privacy europeo (art. 70 del GDPR) fornire indicazioni su come applicare il GDPR in relazione al trattamento personale dei dati tramite dispositivi video**

Le linee guide sono utile strumento per i progettisti, installatori, committenti, lavoratori, cittadini, clienti

Il Comitato europeo conferma che nell'utilizzo dei dispositivi video devono essere applicati i principi del trattamento dei dati personali, di cui all'art 5 del GDPR.

Rischi della videosorveglianza

Oltre ai problemi di privacy, ci 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, il riconoscimento o l'analisi del viso si comporta diversamente in base all'età, al sesso e all'etnia della persona che sta identificando. Gli algoritmi si comporterebbero in base a dati demografici diversi, **pertanto la distorsione nel riconoscimento facciale minaccia di rafforzare i pregiudizi sociali**. Per questo motivo i titolari del trattamento dei dati devono anche garantire che il trattamento dei dati biometrici derivanti dalla videosorveglianza sia sottoposta a una valutazione periodica della sua pertinenza e della adeguatezza delle garanzie fornite.
La videosorveglianza non è di default una necessità quando esistono altri mezzi per raggiungere la finalità sottostante. Altrimenti rischiamo un cambiamento nei modelli culturali che porta all'accettazione della mancanza di privacy come principio generale.

Usa, arrestato per errore riconoscimento facciale

Ong accusa polizia Detroit: stop all'uso di tecnologia razzista

Redazione ANSA

ROMA

26 giugno 2020
16:44

NEWS

Principi del trattamento

Principi fondamentali (5.1)

a) «**liceità, correttezza e trasparenza**» (requisiti del trattamento);

b) «**limitazione della finalità**» (dati raccolti solo per scopi definiti e legittimi);

c) «**minimizzazione dei dati**» (adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati);

d) «**esattezza**» (dati esatti e, se necessario, aggiornati);

e) «**limitazione della conservazione**» (dati conservati in una forma che consenta l'identificazione non oltre il tempo minimo necessario);

f) «**integrità e riservatezza**» (assicurare adeguata sicurezza, compresa la protezione, adottando adeguate misure tecniche e organizzative).

Il titolare** del trattamento è **competente** per il rispetto del par. 1 **e in grado di comprovarlo («responsabilizzazione»). (5.2)

Relazione del Garante « *Prima dell'installazione, è necessario accertare che lo strumento sia proporzionato alla finalità perseguita*».

Liceità del trattamento

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;

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

c) adempimento di un **obbligo legale** al quale è soggetto il titolare del trattamento (*);

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

e) esecuzione di un **compito di interesse pubblico** o connesso all'**esercizio di pubblici poteri** (*);

f) 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.

(*) deve essere stabilita dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

(**) non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti

Gli adempimenti protezione dati personali: un percorso organizzativo (a)

-stabilire chi fa che cosa: quale funzione /ufficio aziendale prende in carico l'installazione, la gestione, la manutenzione, la dismissione degli impianti

-definizione della filiera dell'organigramma privacy con clausole sul rispetto dei principi privacy by design, privacy by default, security by design, data breach, audit

- designazione **dei soggetti autorizzati** (chi può avere accesso alle immagini, la definizione dei profili di autorizzazione)

- **formazione e aggiornamento dei soggetti autorizzati**

-definizione di una procedura nel caso di data breach

- definizione di procedure per l'esercizio dei diritti degli interessati e per le richieste di accesso alle immagini delle autorità

Gli adempimenti protezione dati personali: un percorso organizzativo (b)

- specificare le **finalità del trattamento** ai sensi dell'art. 5, comma 1, lett.b) del regolamento

" i *dati devono essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati in*
modo che non sia incompatibile con tali finalità"
-no a locuzioni generiche: es. per ragioni di sicurezza

- **documentare, per iscritto, nel rispetto del principio di accountability, il rispetto dei principi del**
trattamento previsti dall'art. 5 del GDPR (necessità, proporzionalità,minimizzazione e limitazione
della conservazione), indicare la granularità degli scopi degli impianti

- specificare e documentare la relativa base giuridica del trattamento di videosorveglianza (art. 6 GDPR)

- rilasciare **le informazioni privacy previste dall'art. 13 del GDPR (informativa privacy)**

- adottare misure di sicurezza organizzative e tecniche adeguate (art. 32 GDPR) **stabilire chi fa che cosa**: quale funzione /ufficio aziendale prende in carico l'installazione, la gestione, la manutenzione, la dismissione degli impianti

La trasparenza del trattamento

approccio multilivello

a) **primo di livello** consistente nel segnale di avvertimento, ossia un **cartello raffigurante** la videosorveglianza e che riporti l'identità del titolare del trattamento, del suo rappresentante (art. 27 GDPR), dati di contatto del DPO, le finalità del trattamento, le basi giuridiche e un accenno ai diritti. Il cartello, secondo il Comitato deve essere **posto a una distanza ragionevole dal raggio di azione della telecamera** (prima di entrare nella zona videosorvegliata **ad altezza degli occhi)**

b) **Il secondo livello** consiste nel fornire le informazioni complete sul trattamento come previsto dall'art. 13 del GDPR, in un luogo facilmente accessibile dall'interessato e che non sia nell'area sottoposta a videosorveglianza.

Cosa devono fare le imprese?

Occorre aggiornare la cartellonistica!

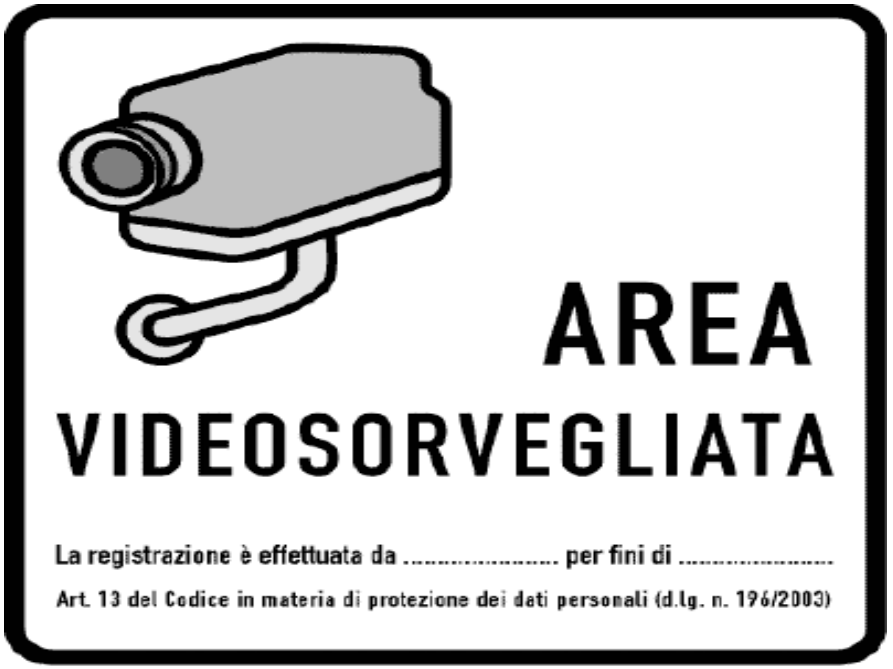
I cartelli che avvisano della presenza di telecamere devono essere aggiornati secondo le Linee guida n. 3/2019 del Comitato Europeo per la protezione dei dati (EDPB) che rappresentano un tassello nell'attuazione del GDPR, il Regolamento Europeo sulla Privacy.

Si tratta di una delle novità più importanti delle Linee guida, ancora in fase di definizione
il nuovo cartello di avviso di videosorveglianza contiene più informazioni rispetto al modello attuale del Garante italiano per la protezione dei dati dell'8 aprile 2010.

Quali informazioni?

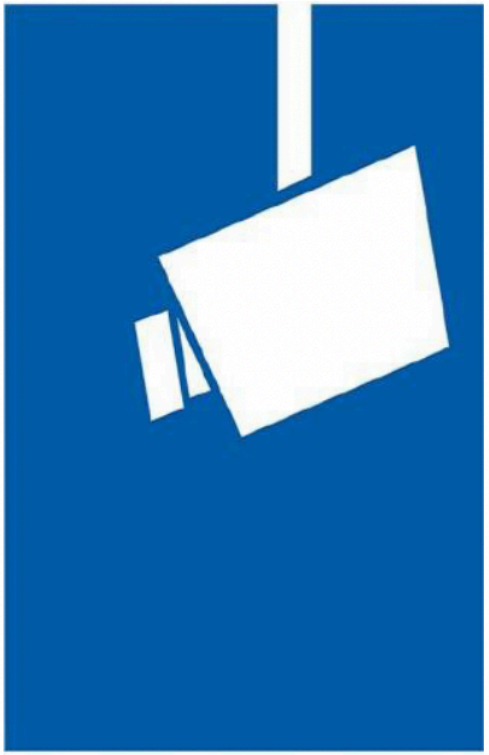
-Finalità del trattamento
-Estremi identificativi del titolare
-Diritti degli interessati
-Dati di contatto del DPO (Data Protection Officer)
-Riferimento al legittimo interesse del titolare o di terze parti o alla base giuridica (nel nostro caso di enti pubblici)
-Codice QR e le modalità che rinviano all'informativa di "secondo livello"
-Eventuale trasferimento di dati extra-UE e il periodo di conservazione delle immagini

Il cartello Modello semplificato del Garante privacy del 201 va in pensione



Il Nuovo cartello

Esempio (suggerimento non vincolante):



Videosorveglianza!

Identità del titolare e, ove applicabile, del rappresentante del titolare:

Dati di contatto, incluso del responsabile della protezione dei dati (ove applicabile):

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

Finalità della videosorveglianza:

Ulteriori informazioni sono disponibili:

- tramite avviso
- presso la nostra receptionr/ informazione clienti/ registri
- via internet (URL)...

Diritti degli interessati: In qualità di interessato hai diversi diritti da esercitare, in particolare il diritto di richiedere al titolare del trattamento l'accesso o la cancellazione dei tuoi dati personali.

Per i dettagli su questa videosorveglianza, compreso i tuoi diritti, consulta le informazioni complete fornite dal titolare per mezzo delle opzioni presentate a sinistra.

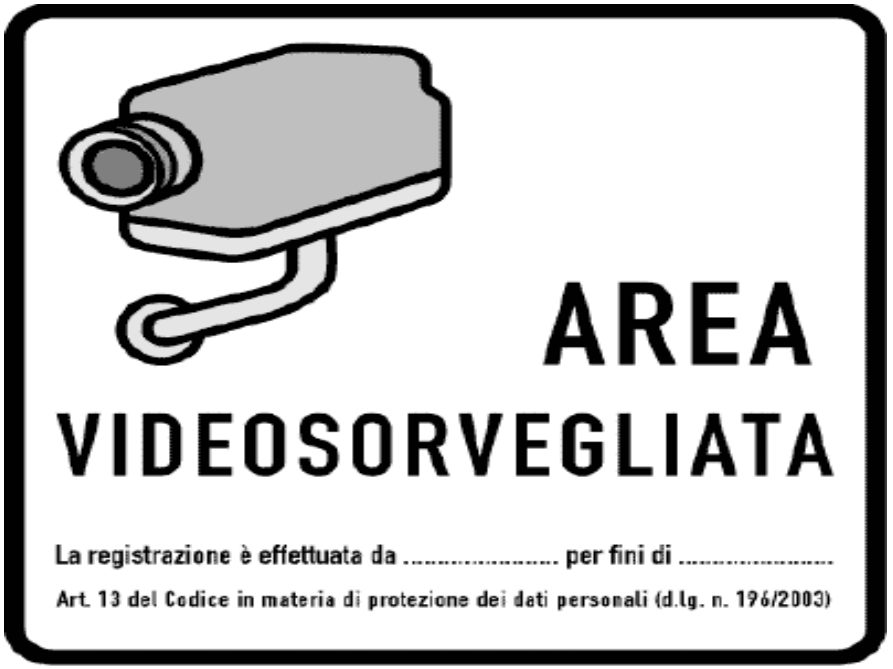
Cosa devono fare le imprese?

Occorre aggiornare la cartellonistica!

I cartelli che avvisano della presenza di telecamere devono essere aggiornati secondo le Linee guida n. 3/2019 del Comitato Europeo per la protezione dei dati (EDPB) che rappresentano un tassello nell'attuazione del GDPR, il Regolamento Europeo sulla Privacy.

Si tratta di una delle novità più importanti delle Linee guida, ancora in fase di definizione
il nuovo cartello di avviso di videosorveglianza contiene più informazioni rispetto al modello attuale del Garante italiano per la protezione dei dati dell'8 aprile 2010.

Il cartello Modello semplificato del Garante privacy del 201 va in pensione



Grazie per attenzione!

Avv. Mauro Alovisio
Università degli Studi di Torino

3333597588

Presidente Csig Ivrea Torino www.csigivreatorino.it

Fellow Nexa

per approfondimenti: mauro.alovisio@gmail.com

LinkdIn: Mauro Alovisio
Twitter: Mauro Alovisio

Per approfondimenti

Mauro Alovisio, (curatore) «*Videosorveglianza e GDPR. Profili di compliance nelle imprese e nelle pubbliche amministrazioni*» , Giuffrè, 2021

Mauro Alovisio, ‘‘*Videosorveglianza in ambito pubblico*” in “Videosorveglianza e privacy Experta Edizioni, settembre 2011

Anna Capoluongo, *Videosorveglianza Game Changer*, 2021

Autori vari, *The Law of Service Robots* , Centro Nexa 2015

Biasotti, *Gli impianti di videosorveglianza, Progettazione, gestione, manutenzione, protezione dei dati*, Epc, 2019

Alessandro Del Ninno, *La proposta di Regolamento UE sull’intelligenza Artificiale: i profili operativi del nuovo quadro normativo europeo;* Diritto e Giustizia 2021

Francesco Pizzetti, Protezione dei dati personali in Italia fra GDPR e codice novellato, Giappichelli 2021

Pierluigi Perri , *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffrè 2021

Stefano Manzelli, Videocontrollo urbano: il grande fratello bussa alle porte del municipio, Diritto e Giustizia, 2020

Paola Zanellati, Dati biometrici, ecco come vanno trattati in ambito lavorativo, 2021 , Cyberlaw, 2021

Videosorveglianza

Domande più frequenti (FAQ)

Footer

- Informativa protezione dati
- Link utili
- Mappa del sito
- Regole del sito
- Iscrizione alla Newsletter
- Urp e servizi utili

SCARICA LE FAQ IN FORMATO .PDF

Faq

1 Quali sono le regole da rispettare per installare sistemi di videosorveglianza?

2 Occorre avere una autorizzazione da parte del Garante per installare le telecamere?

Grazie per attenzione!

Avv. Mauro Alovisio
Università degli Studi di Torino

3333597588

Presidente Csig Ivrea Torino www.csigivreatorino.it

Fellow Nexa

per approfondimenti: mauro.alovisio@gmail.com

LinkdIn: Mauro Alovisio
Twitter: Mauro Alovisio