Videosorveglianza e privacy - La nuova videosorveglianza alla luce del Regolamento europeo

Marco Soffientini

Avvocato, esperto di Privacy e Diritto delle nuove Tecnologie, docente Ethos Academy

Silvia Mencaroni

Esperto di Privacy, docente Ethos Academy

Validato da TÜV Italia

Evento favorito da

Milesight

STRUTTURA DELLA PRESENTAZIONE

La responsabilità

- Le nuove Norme
- Accountability

Tecnologia

- L'acquisizione di immagini
- Face Detection e face recognition

Come Tutelarsi

- DPIA
- DPO

25 Maggio 2018 - 08 Maggio 2019

Dati riferiti al periodo 25 maggio 2018 - 31 marzo 2019

RGPD
REGOLAMENTO (UE) 2016/679

Il bilancio dell'applicazione

(Periodo: 25 maggio 2018 – 31 marzo 2019)

Comunicazioni dei dati di contatto degli RPD **48.591**

Reclami e segnalazioni **7.219**

Notifiche di Data Breach **946**

Contatti con l'URP **18.557**

www.garanteprivacy.it

RGPD
REGOLAMENTO (UE) 2016/679

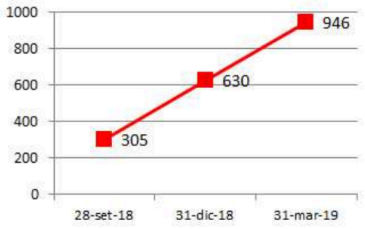
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il bilancio dell'applicazione

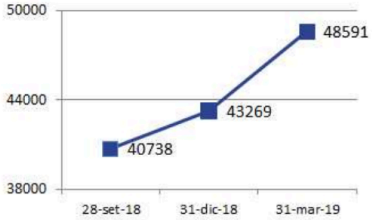
I grafici mostrano l'andamento nel periodo compreso tra il 28 settembre 2018 (data del primo bilancio applicativo diffuso sul sito del Garante) e il 31 marzo 2019.

Reclami e segnalazioni

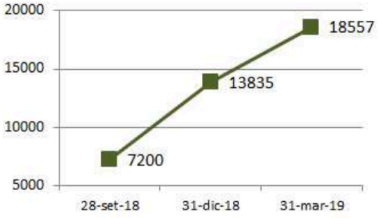
Notifiche di data breach



Comunicazioni dei dati di contatto degli RPD



Contatti con l'URP



www.garanteprivacy.it

07 Maggio 2019
Relazione Annuale

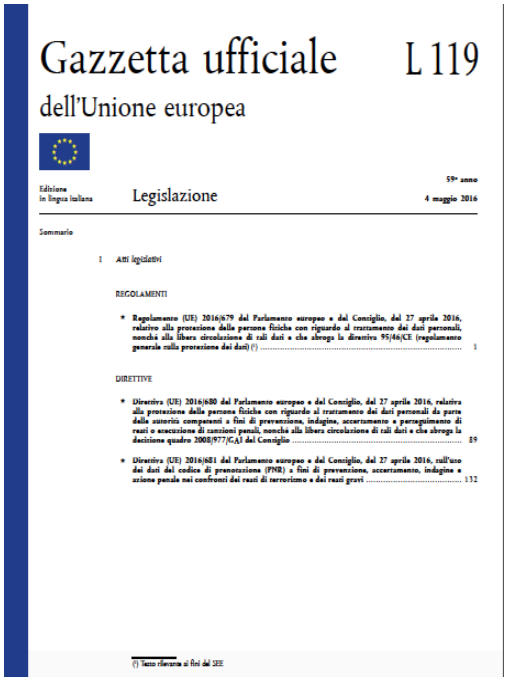
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

«Le nuove tecnologie, che hanno consentito straordinarie e irrinunciabili conquiste per l'umanità, hanno progressivamente trasferito nello spazio digitale una parte significativa delle attività private e pubbliche».

07.05.2019: Relazione Annuale 2018 – Discorso del Presidente Autorità Garante

REGOLAMENTO UE 2016/679

GENERAL DATA PROTECTION REGULATION – GDPR -



Gazzetta ufficiale L 119
dell'Unione europea

Edizione in lingua italiana — Legislazione — 59° anno — 4 maggio 2016

Sommario

I Atti legislativi

REGOLAMENTI

* 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 (regolamento generale sulla protezione dei dati) (1) 1

DIRETTIVE

* Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio 89

* Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi 132

(1) Testo rilevante ai fini del SEE

Il Regolamento Europeo sul trattamento dei dati personali UE 2016/679 ABROGA la direttiva a decorrere dal 25 maggio 2018, data a partire dalla quale il Regolamento è pienamente applicabile (art.95, co.1 e 99,co.2 Reg. UE 2016/679).

SANZIONI –ART. 83 -

SOCIAL E MINORI –ART. 8 -

DIRITTO ALL'OBLIO –ART. 17 -

Diritto alla portabilità dei dati – ART. 20 -

RESPONSABILITA' VERIFICABILE – ART. 5.2 -

Diritto di accesso dell'interessato – ART. 15 -

Registro delle attività di trattamento – ART. 30 -

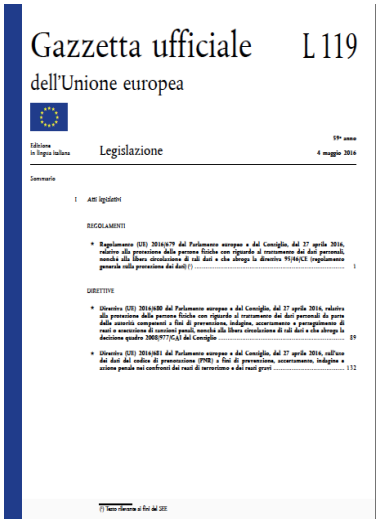
Notifica di una violazione dei dati personali – ART. 33 -

Meccanismo dello sportello unico (One stop shop) – ART. 60 -

Designazione del responsabile della protezione dei dati –ART. 37 -

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI – ART. 35 -

Protezione dei dati fin dalla progettazione e per impostazione predefinita – ART. 25 -


Gazzetta ufficiale L 119
dell'Unione europea

Edizione in lingua italiana — Legislazione — 59° anno — 4 maggio 2016

Sommario

I Atti legislativi

REGOLAMENTI

• 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 (regolamento generale sulla protezione dei dati) (1) 1

DIRETTIVE

• Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio 89

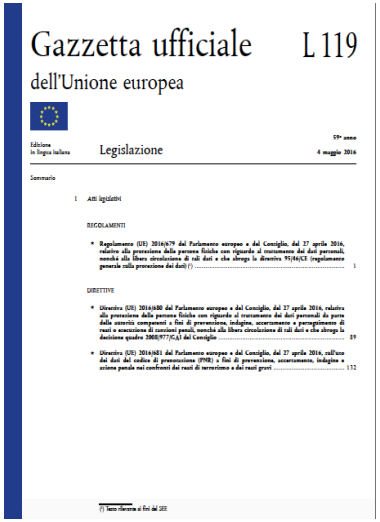
• Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi 132

(1) Testo rilevante ai fini del SEE

Perché è importante capire cos'è il principio di **accountability**

IL PRINCIPIO DELL'ACCOUNTABILITY

Il principio dell'accountability o di responsabilizzazione consiste nel dovere del titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate al fine di dimostrare che il trattamento è effettuato conformemente al regolamento.


Gazzetta ufficiale L 119
dell'Unione europea

Legislazione

DIRETTIVA 2016/680

Per quanto concerne la direttiva (UE) 2016/680, bisogna evidenziare come essa abbia natura di lex specialis rispetto al regolamento generale sulla protezione dei dati, di cui declina princìpi e obblighi con riguardo allo specifico contesto di attività e ai poteri delle autorità di polizia e giudiziarie.

La DIRETTIVA 2016/680 del Parlamento europeo e del Consiglio d'Europa sulla protezione delle persone fisiche con riferimento al TRATTAMENTO DEI DATI da parte delle autorità a fini di prevenzione, investigazione e repressione di reati è entrata in vigore il 5 maggio 2016 e si attua dal 6 maggio 2018. La direttiva unifica le norme sulla **cooperazione transfrontaliera delle forze di polizia e in materia di giustizia**.

D.lgs 18 Maggio 2018, n. 51

G.U. 24.05.2018, Serie generale n.119
In vigore dal 08 giugno 2018

Il decreto regolamenta il trattamento dei dati personali per finalità di prevenzione e repressione di reati, esecuzione di sanzioni penali, salvaguardia contro le minacce alla sicurezza pubblica e prevenzione delle stesse, da parte sia dell'autorità giudiziaria, sia delle forze di polizia.

CODICE DELLA PRIVACY

Modificato dal D.Lgs 10 Agosto 2018, n.101

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DECRETO LEGISLATIVO 30 giugno 2003, n.196
recante il "Codice in materia di protezione dei dati personali"
(in S.O n. 123 alla G.U. 29 luglio 2003, n. 174)

integrato con le modifiche introdotte dal

DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni 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, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"
(in G.U. 4 settembre 2018 n.205)

1

Il nuovo Codice della Privacy (D.Lgs n.196/2003) così come modificato dal D.Lgs 10 Agosto 2018, n.101 è entrato in vigore il 19 Settembre 2018.

VIDEOSORVEGLIANZA:LE PRINCIPALI FONTI NORMATIVE

REGOLAMENTO UE 2016/679


DIRETTIVA 680/2016 – D.LGS 51/2018

D.LGS 196/2003 come modificato D.Lgs 101/2018

STATUTO DEI LAVORATORI – L. n.300/1970

Provv. Generale 08 aprile 2010, doc. web n. 1712680.

Il primo aspetto da tenere presente nell'approccio al Regolamento (UE) n. 2016/679 "General Data Protection Regulation, c.d. GDPR, è che la norma non pone più al centro il dato come nel d.lgs. 196/2003, bensì il **TRATTAMENTO**, cioè l'utilizzo che si pone in essere del medesimo e che deve sempre trovare fondamento in un'idonea base giuridica

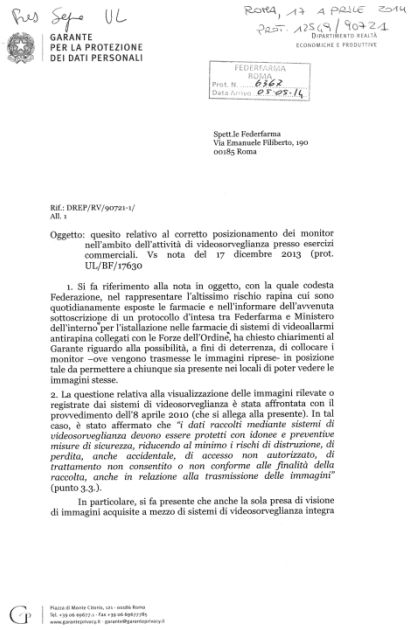
Trattamento

TRATTAMENTO: Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.

Il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini. (§ 3.3.2 Provv. 08.04.2010).

SI PUO' INSTALLARE ALL'INTERNO DI UN ESERCIZIO COMMERCIALE UN MONITOR CHE CONSENTA LA VISIONE DELLE IMMAGINI A CHIUNQUE SIA PRESENTE NEI LOCALI ?

"Anche la sola presa di **visione** di immagini acquisite a mezzo di sistemi di videosorveglianza integra un **trattamento** di dati personali. Pertanto, i dati rilevati – e cioè le immagini trasmesse su un monitor – devono essere oggetto di protezione, sicché la loro visione deve essere **riservata** soltanto a coloro che, nominati previamente dal titolare del trattamento dei dati "**incaricati**", ai sensi dell'art. 30 del Codice, abbiano il compito di controllare le stesse per evitare la consumazione di possibili illeciti. **Ne consegue che non può ritenersi conforme a legge una visione delle immagini "generalizzata", che non solo non sia limitata ai soggetti effettivamente titolati a prenderne visione, ma addirittura si estenda a "chiunque sia presente nei locali dell'esercizio commerciale o della farmacia**"



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Roma, 17 APRILE 2014

Spett.le Federfarma
Via Emanuele Filiberto, 190
00185 Roma

Rif.: DREP/RV/90721-1/
All. 1

Oggetto: quesito relativo al corretto posizionamento dei monitor nell'ambito dell'attività di videosorveglianza presso esercizi commerciali. Vs nota del 17 dicembre 2013 (prot. UL/BF/17630

1. Si fa riferimento alla nota in oggetto, con la quale codesta Federazione, nel rappresentare l'altissimo rischio rapina cui sono quotidianamente esposte le farmacie e nell'informare dell'avvenuta sottoscrizione di un protocollo d'intesa tra Federfarma e Ministero dell'interno per l'istallazione nelle farmacie di sistemi di videoallarmi antirapina collegati con le Forze dell'Ordine, ha chiesto chiarimenti al Garante riguardo alla possibilità, a fini di deterrenza, di collocare i monitor –ove vengono trasmesse le immagini riprese- in posizione tale da permettere a chiunque sia presente nei locali di poter vedere le immagini stesse.

2. La questione relativa alla visualizzazione delle immagini rilevate o registrate dai sistemi di videosorveglianza è stata affrontata con il provvedimento dell'8 aprile 2010 (che si allega alla presente). In tal caso, è stato affermato che *"i dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini"* (punto 3.3.).

In particolare, si fa presente che anche la sola presa di visione di immagini acquisite a mezzo di sistemi di videosorveglianza integra

VEDI NOTA GARANTE
17 APRILE 2014

L'INFORMATIVA BREVE NELLA VIDEOSORVEGLIANZA

IL GARANTE HA INDIVIDUATO AI SENSI DELL'ART. 13, COMMA 3, DEL CODICE, L'UTILIZZO DI UN MODELLO SEMPLIFICATO DI INFORMATIVA MINIMA, INDICANTE IL TITOLARE DEL TRATTAMENTO E LA FINALITA' PERSEGUITA.

§ 3.1 PROVV. 08.04.2010

Questo fac-simile può essere utilizzato dai soggetti privati che effettuano trattamenti di dati personali effettuati tramite sistemi di videosorveglianza direttamente collegati con le forze di polizia.

Afferma il provv. 08.04.2010 che questo tipo di collegamento DEVE ESSERE RESO NOTO AGLI INTERESSATI. (vedi § 3.1.3. provv. 08.04.2010)

L'INFORMATIVA BREVE NELLA VIDEOSORVEGLIANZA

In presenza di più telecamere, in relazione alla vastità dell'area oggetto di rilevamento e alle modalità delle riprese, **potranno essere installati più cartelli**.

Il supporto con l'informativa:

- **deve essere collocato prima del raggio di azione della telecamera**, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;

- **deve avere un formato ed un posizionamento tale da essere chiaramente visibile** in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;

- **può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione**, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Provv. 08.04.2010, § 3.1.

"L'installazione di un impianto di videosorveglianza all'interno di un esercizio commerciale, costituendo trattamento di dati personali, deve formare oggetto di previa informativa, ex art. 13 del d.lgs. n. 196 del 2003, resa ai soggetti interessati prima che facciano accesso nell'area videosorvegliata, mediante supporto da collocare perciò fuori del raggio d'azione delle telecamere che consentono la raccolta delle immagini delle persone e danno così inizio al trattamento stesso". (Cass. 5 luglio 2016, n. 13663).

Naturalmente occorre ricordarsi di compilare la cartellonistica, con l'indicazione del titolare del trattamento e la finalità della rilevazione/registrazione.

E SE IL LAVORATORE SI RIFIUTA DI SOTTOSCRIVERE LA DESIGNAZIONE ?

Osserva il GARANTE che:

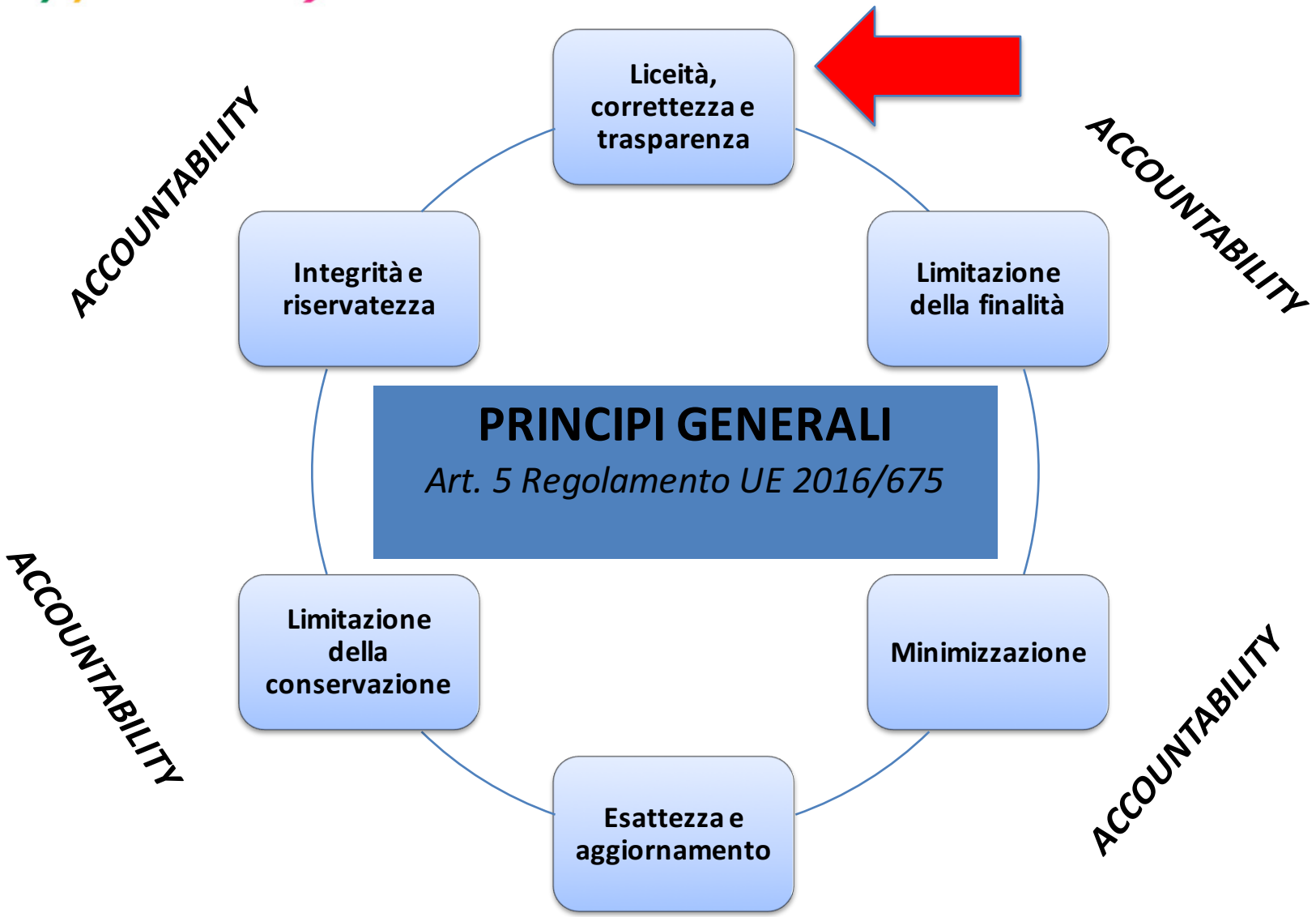
Senza una formale designazione degli incaricati del trattamento (Con il Regolamento UE 2016/679 “soggetti autorizzati ex art. 4. N.10 GDPR), i dipendenti che, per lo svolgimento dei propri compiti, vengono a conoscenza di dati personali dovrebbero essere considerati come soggetti terzi, rispetto al titolare, con conseguenti rilevanti limiti per la comunicazione e l´utilizzazione dei dati e quindi per la liceità del trattamento.

tale designazione non comporta l´attribuzione di particolari compiti o responsabilità in capo al personale, ma c**ostituisce un riconoscimento della legittimità delle operazioni di trattamento di dati collegate all´ufficio a cui il dipendente risulta assegnato** e alle specifiche mansioni ad esso attribuite, chiarendo per ogni impiegato quali sono le informazioni cui può avere accesso e rafforzando i già previsti obblighi del segreto d´ufficio.

L' autorizzazione al trattamento è un atto di "riconoscimento", il cui perfezionamento non è subordinato alla espressione di una volontà adesiva da parte del dipendente. Per queste ragioni la firma va raccolta "per ricevuta" o per "presa visione" e anche qualora sia omessa la designazione produce i suoi effetti.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nota 23 maggio 2000, indirizzata all'Anci (doc. web n. 40229).


Liceità, correttezza e trasparenza
Limitazione della finalità
Minimizzazione
Esattezza e aggiornamento
Limitazione della conservazione
Integrità e riservatezza
PRINCIPI GENERALI
Art. 5 Regolamento UE 2016/675
ACCOUNTABILITY
ACCOUNTABILITY
ACCOUNTABILITY
ACCOUNTABILITY

PERCHE' IL TEMA DELLA PRIVACY E' STATA OGGETTO DI UNA PROFONDA REVISIONE NORMATIVA ?

L'EVOLUZIONE TECNOLOGICA
(Nella Videosorveglianza)

IMPATTO PRIVACY


Gazzetta ufficiale L 119
dell'Unione europea
Legislazione

COSA DICE IL REGOLAMENTO UE 2016/679

La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. (CONSIDERANDO N. 6)

al fine di «*assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possano ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto*». (CONSIDERANDO N. 13).

Cellulare – Telefonino - Smartphone

Videosorveglianza

Internet

L'Italia è il terzo Paese al mondo (dopo Corea del Sud e Hong Kong) per numero di telefonini

Il 76% della popolazione italiana usa uno smartphone.

I messaggi sono la principale attività svolta con lo smartphone.

Il 61% della popolazione scrive **messaggi** da dispositivi mobili

il 45% usa lo smartphone per fare **foto**,

il 52% lo usa per vedere **video** e

il 31% legge le informazioni meteo.

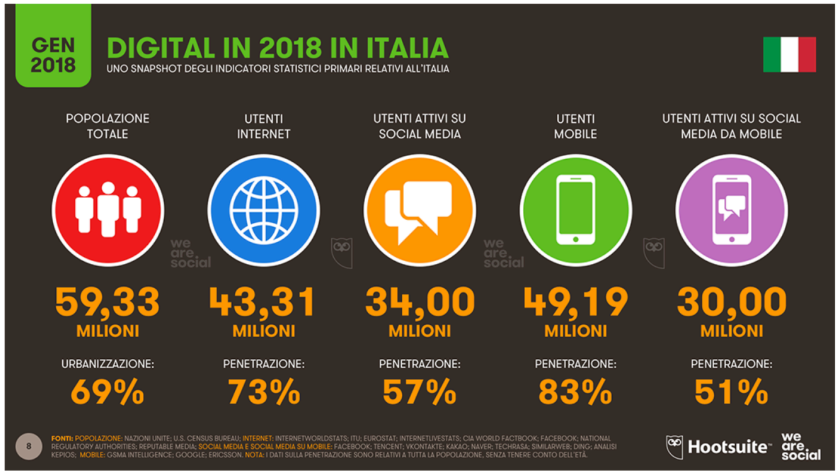
I messaggi sono quindi al primo posto tra le funzioni quotidiane dello smartphone.

WhatsApp: l'applicazione di messaggistica più popolare in Italia: il 59% della popolazione italiana usa WhatsApp.

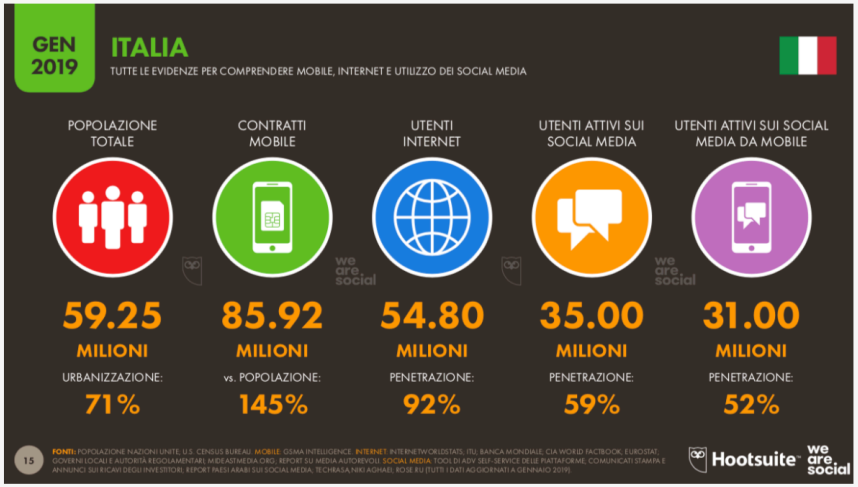
FONTE: https://wearesocial.com/it/blog/2019/01/digital-in-2019

Fonte: https://www.messengerpeople.com/it/messaggistica-in-italia-whatsapp-rappresenta-il-951-del-mercato/

Sono quasi 55 milioni gli italiani ad accedere ad internet



Passiamo oltre 6 ore al giorno connessi (di cui circa un terzo sui social)



FONTE: https://wearesocial.com/it/blog/2019/01/digital-in-2019

E la Videosorveglianza ?

Uno **smartphone** viene utilizzato come **telecamera di sicurezza** da parte di molti privati: un sensore fotografico versatile, sensori di movimento di ultima generazione e **connettività web** ad alta velocità.

Per trasformare lo smartphone in **telecamera IP di sicurezza**, è sufficiente installare un'app che sia in grado di "coordinare" le varie operazioni e sfruttare al meglio sensori fotografici e sensori di movimento installati nel dispositivo.

L'ANGOLO DI VISUALE DELLE TELECAMERE

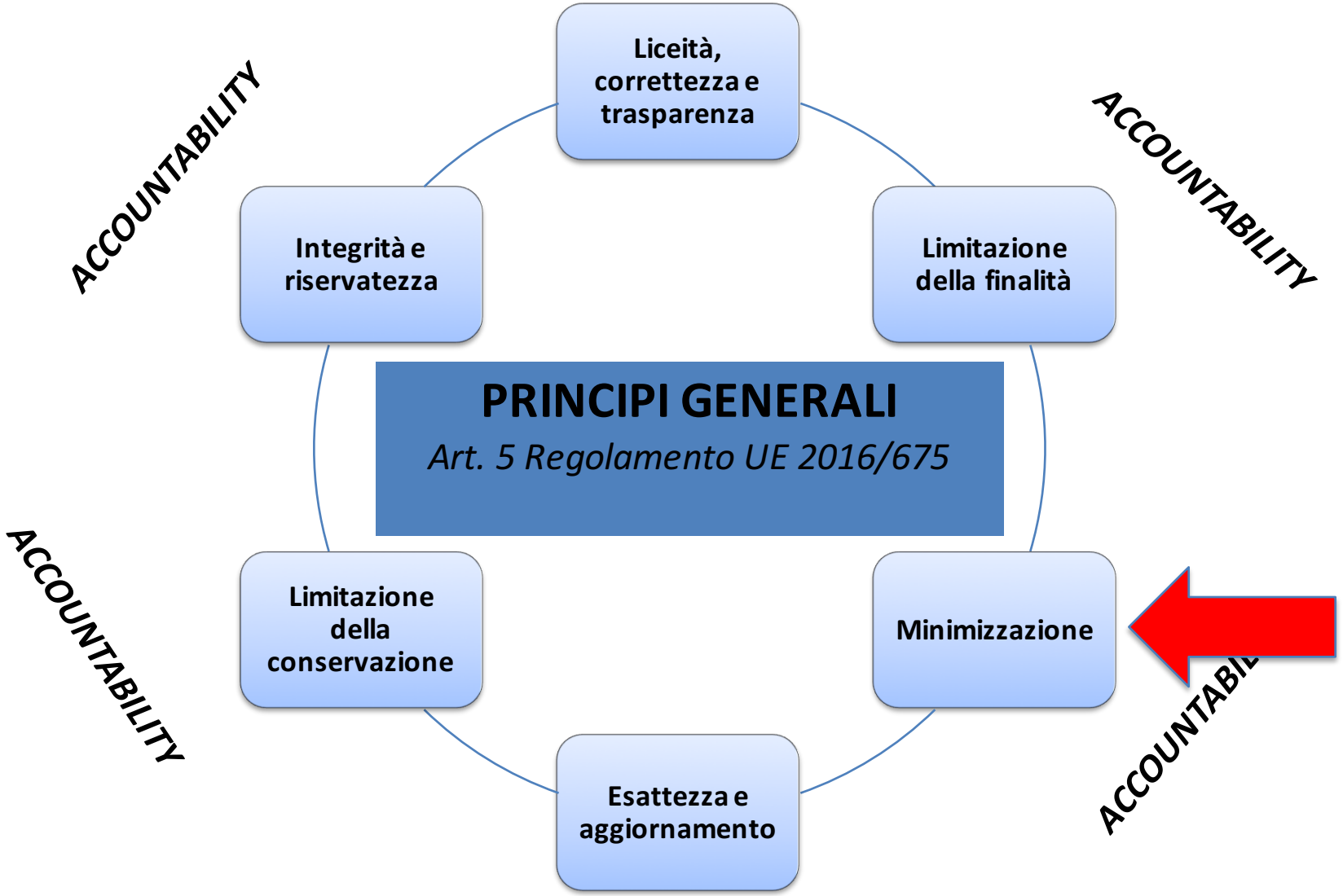
Posso Riprendere spazi pubblici ?

Può l'esercizio commerciale installare una telecamera che riprenda non solo l'ingresso ma l'intera strada pubblica ?

Aziende, Ristoranti, Bar, Aree di Servizio, Esercizi Commerciali, ecc.

Nell´uso delle apparecchiature volte a riprendere, con o senza registrazione delle immagini, aree esterne ad edifici e immobili (perimetrali, adibite a parcheggi o a carico/scarico merci, accessi, uscite di emergenza), resta fermo che il trattamento debba essere effettuato con modalità tali da limitare l´angolo visuale all´area effettivamente da proteggere, evitando, per quanto possibile, la ripresa di luoghi circostanti e di particolari che non risultino rilevanti (vie, edifici, esercizi commerciali, istituzioni ecc.).

Provv. 08.04.2010, § 6.2.2.1


Liceità, correttezza e trasparenza
Limitazione della finalità
Minimizzazione
Esattezza e aggiornamento
Limitazione della conservazione
Integrità e riservatezza
PRINCIPI GENERALI
Art. 5 Regolamento UE 2016/675
ACCOUNTABILITY
ACCOUNTABILITY
ACCOUNTABILITY
ACCOUNTABILITY

E per la Videosorveglianza a casa dei privati ?

6.1. Trattamento di dati personali per fini esclusivamente personali

L´installazione di sistemi di videosorveglianza -come si rileva dall´esame di numerose istanze pervenute all´Autorità- viene sovente effettuata da persone fisiche per fini esclusivamente personali. In tal caso va chiarito che la disciplina del Codice non trova applicazione qualora i dati non siano comunicati sistematicamente a terzi ovvero diffusi, risultando comunque necessaria l´adozione di cautele a tutela dei terzi (*art. 5, comma 3*, del Codice, che fa salve le disposizioni in tema di responsabilità civile e di sicurezza dei dati). In tali ipotesi possono rientrare, a titolo esemplificativo, strumenti di videosorveglianza idonei ad identificare coloro che si accingono ad entrare in luoghi privati (videocitofoni ovvero altre apparecchiature che rilevano immagini o suoni, anche tramite registrazione), oltre a sistemi di ripresa installati nei pressi di immobili privati ed all´interno di condomini e loro pertinenze (quali posti auto e *box*).

Benché non trovi applicazione la disciplina del Codice, al fine di evitare di incorrere nel reato di interferenze illecite nella vita privata (*art. 615-bis c.p.*), l´angolo visuale delle riprese deve essere comunque limitato ai soli spazi di propria esclusiva pertinenza (ad esempio antistanti l´accesso alla propria abitazione) escludendo ogni forma di ripresa, anche senza registrazione di immagini, relativa ad aree comuni (cortili, pianerottoli, scale, garage comuni) ovvero ad ambiti antistanti l´abitazione di altri condomini.

Provv. 08.04.2010, § 6.1

LA VALUTAZIONE DI IMPATTO PRIVACY (DPIA) NELLA VIDEOSORVEGLIANZA

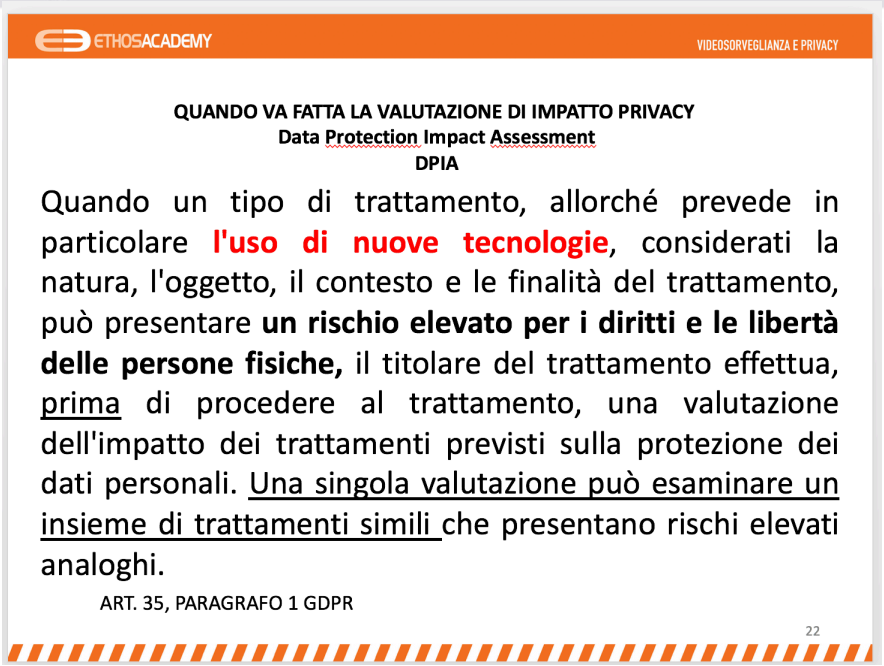
IMPATTI PRIVACY (E NON SOLO) NELL'UTILIZZO DELLE TELECAMERE

~~VERIFICA PRELIMINARE~~

DPIA

Con la piena attuazione del GDPR l'intervento delle autorità di controllo avviene principalmente "ex post", ossia si colloca successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega **l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano**, come la **notifica preventiva dei trattamenti** all'autorità di controllo e il cosiddetto *prior checking* (o verifica preliminare: si veda art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e di effettuazione di valutazioni di impatto in piena autonomia.

OBIETTIVO DELLA DPIA



Rispettare i «PRINCIPI»

GESTIRE I «RISCHI»

La DPIA è un processo sistematico che consente di valutare la **liceità**, **necessità** e **proporzionalità** del trattamento e di valutare e **gestire i rischi** incombenti per i diritti e le libertà delle persone fisiche i cui dati personali sono trattati.

il 45% della popolazione italiana usa lo smartphone per fare **foto**, mentre il 52% lo usa per vedere **video**

FOTO E VIDEO ONLINE

Osserva il Garante:

Rifletti bene prima di postare online foto o filmati. Potrebbe poi essere molto difficile eliminarli, soprattutto se qualcuno li ha copiati, condivisi, o diffusi su altri siti o social network.

Registrare o riprendere una persona a Sua insaputa è legale ?

Registrare di nascosto quello che dice una persona è reato ? E se invece del registratore si utilizza una **telecamera** e, pertanto, oltre alle voci, a finire nell'obiettivo indiscreto sono anche i volti ?

Corte di Cassazione, sez. II Penale 10 giugno 2016, n. 24288

La registrazione di conversazione tra presenti, compiuta di propria iniziativa da uno degli interlocutori, anche come spettatore, non richiede l'autorizzazione del giudice e può essere usata in processo.

Le registrazioni di conversazioni tra presenti, compiute di propria iniziativa da uno degli interlocutori, non necessitano dell'autorizzazione del giudice per le indagini preliminari, ai sensi dell'art. 267 c.p.p., in quanto non rientrano nel concetto di intercettazione in senso tecnico, ma si risolvono in una particolare **forma di documentazione, che non è sottoposta alle limitazioni ed alle formalità proprie delle intercettazioni.**

Al riguardo le Sezioni Unite hanno evidenziato che, in caso di registrazione di un colloquio ad opera di una delle persone che vi partecipi attivamente o che sia comunque ammessa ad assistervi, difettano la compromissione del diritto alla segretezza della comunicazione, il cui contenuto viene legittimamente appreso soltanto da chi palesemente vi partecipa o vi assiste, e la "terzietà" del captante. L'acquisizione al processo della registrazione dei colloquio può legittimamente avvenire attraverso il meccanismo di cui all'art. 234 c.p.p., comma 1, che qualifica documento tutto ciò che rappresenta fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo; il nastro contenente la registrazione non è altro che la documentazione fonografica dei colloquio, la quale può integrare quella prova che diversamente potrebbe non essere raggiunta e può rappresentare (si pensi alla vittima di un'estorsione) una forma di autotutela e garanzia per la propria difesa, con l'effetto che una simile pratica finisce col ricevere una legittimazione costituzionale" (Cass. Sez. Un. 28-5-2003 n. 36747).

Cass. Penale, 28 novembre 2007, n.1766

Riprendere una persona a sua insaputa è legale solo a condizione che chi usa la telecamera sia presente.

L'importante – dicono i giudici supremi – è che il proprietario della telecamera sia presente e non, invece, da un'altra parte. In altre parole la **ripresa video è legale anche se una persona non lo sa** a condizione che chi filma sia partecipe. Non è lecito invece lasciare la telecamera accesa e andare in un'altra stanza, facendo ritenere a chi invece rimane di essere solo.

Al pari di chi registra una conversazione all'insaputa degli altri partecipanti alla discussione non commette reato.

Non è la «privatezza» della scena ripresa ad essere il punto di confine tra il lecito e l'illecito quando si decide di fare una **ripresa video all'insaputa dell'altro**, bensì la circostanza che il soggetto attivo sia o meno estraneo alla scena.

?

Può essere denunciato chi, a casa propria, riprende (con una telecamera tradizionale o uno smartphone) in segreto una notte d'amore con un'altra persona all'insaputa di questa e quindi senza consenso?

IL FATTO:

Il quesito è stato affrontato dalla Corte di Cassazione che, ha trattato il caso di un uomo che, dopo aver invitato una donna a casa propria e aver trascorso una notte d'amore, ha registrato il tutto con una telecamera nascosta, e ovviamente, senza dirle nulla.

L'uomo si è poi vantato dell'episodio con gli amici e uno di questi ha fatto la spia.

La voce è arrivata alla diretta interessata che non ha avuto alcun dubbio a sporgere querela.

PREMESSA DI DIRITTO

Abbiamo visto che, è lecito **registrare una conversazione** con altre persone o **registrare con una telecamera**, anche se i presenti lo ignorano.

Non è necessario avere il consenso altrui, ma a patto di non essere in un luogo di privata dimora dei soggetti "registrati" e che chi registra non si allontani dalla scena.

Filmare un momento di estrema intimità integra il reato di **interferenza illecita nella vita privata ?**

Corte di Cassazione, sez. V Penale, 13 giugno 2018, n. 27160

Non si configura il reato di **interferenza illecita nella vita privata** se l'uomo invita a casa una donna e filma l'amplesso senza consenso di questa. L'importante è che il proprietario della telecamera sia nella propria dimora e sia una delle persone che partecipa alla scena.

La norma del codice penale **[615 c.p.]** ricollega l'illecito penale della registrazione all'intimità del domicilio violata e non all'assenza di consenso dell'interessata; né rileva la natura dell'azione che si sta svolgendo dentro l'appartamento. Tanto è vero che la norma è stata collocata, dal legislatore, nella parte del codice che persegue i delitti contro l'inviolabilità del domicilio e non quelli della libertà della sfera

Il reato scatterebbe, dicono i giudici nel caso di una persona che registri immagini in un domicilio che non è il proprio.
Questa Corte, infatti, ha già avuto modo di precisare che non integra il reato di interferenze illecite nella vita privata la condotta di colui che mediante l'uso di strumenti di ripresa visiva provveda a filmare in casa propria rapporti intimi intrattenuti con la convivente, in quanto l'interferenza illecita prevista e sanzionata dal predetto articolo è quella proveniente dal terzo estraneo alla vita privata, e non già quella del soggetto che, invece, sia ammesso a farne parte, sia pure estemporaneamente, mentre è irrilevante l'oggetto della ripresa, considerato che il concetto di "vita privata" si riferisce a qualsiasi atto o vicenda della persona in luogo riservato (da ultimo, Sez. 5, n. 22221 del 10/01/2017, Rv. 270236 ed ancor prima Sez. 5, n. 1766 del 28/11/2007, Radicella Chiaromonte, Rv. 239098).

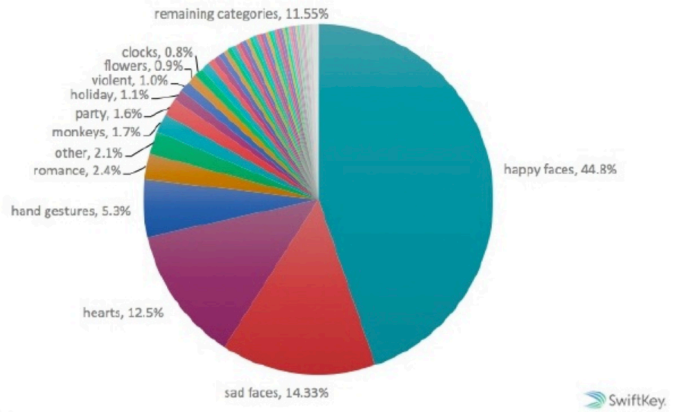
Cass. Penale, 10 gennaio 2017, n. 22221

Cass. Penale, 28 novembre 2007, n.1766

EMOTICON E VIOLAZIONE DELLA PRIVACY

I messaggi sono la principale attività svolta con lo smartphone. Il 61% della popolazione italiana scrive **messaggi** da dispositivi mobili.

Le faccine di gran lunga più utilizzate sono quelle **sorridenti** con ben il **44% di utilizzo**, seguite dalle emoticon tristi.



FONTE: https://www.fastweb.it/smartphone-e-gadget/le-emoticons-piu-utilizzate/

PROVV. 13 DICEMBRE 2018

Nella bacheca aziendale le foto dei lavoratori e un emoticon con il giudizio sull'attività svolta.

"Faccine" e punteggi associati ai volti dei lavoratori nella bacheca aziendale.

Era questo il sistema adottato da una cooperativa toscana che opera nel settore della logistica (pulizie, facchinaggio, traslochi) per valutare l'attività dei propri dipendenti. Ogni settimana la cooperativa affiggeva nella bacheca aziendale un cartello nel quale i volti dei dipendenti erano associati a emoticon che rappresentavano i giudizi, positivi o negativi, espressi dalla cooperativa. Nella bacheca erano affisse anche le eventuali contestazioni disciplinari. Un tale uso dei dati personali dei lavoratori è illecito perché lede la loro dignità, la loro libertà e la loro riservatezza.

Lo ha stabilito il Garante per la privacy che ha vietato all'azienda di proseguire il trattamento dei dati dei dipendenti. Dagli accertamenti avviati dall'Autorità su segnalazione di alcuni lavoratori è emerso che la cooperativa aveva messo in atto una sorta di "concorso a premi" obbligatorio per i lavoratori, con relativo prelievo mensile dalla busta paga della quota di partecipazione, e pubblicava nella bacheca aziendale le valutazioni settimanali sull'attività di ciascun dipendente, cui corrispondevano l'attribuzione di un punteggio valido per il concorso, nonché le eventuali contestazioni disciplinari.

Le valutazioni, espresse con **sei diverse tipologie di emoticon** e con giudizi sintetici quali “assenteismo”, “simulazione malattia”, “perdita di lavoro causa scarso servizio o danni”, oppure l’espressione “licenziato”, comparivano accanto alle foto dei dipendenti individuati con cognome e iniziale del nome.

La valutazione negativa comportava una decurtazione dallo stipendio.

Nel disporre il divieto il Garante ha ricordato che il datore di lavoro può trattare le informazioni necessarie e pertinenti per la gestione del rapporto di lavoro in base a quanto previsto dalle leggi, dai regolamenti, dai contratti collettivi e dal contratto di lavoro individuale. Tra questi rientrano senza dubbio i dati necessari ad effettuare la valutazione sul corretto adempimento della prestazione lavorativa e ad esercitare il potere disciplinare nei modi e nei limiti previsti dalla disciplina di settore.

Ma non certo la sistematica messa a disposizione sulla bacheca aziendale delle valutazioni e dei rilievi disciplinari a tutti i dipendenti e ad eventuali visitatori, tutti soggetti non legittimati a conoscere questo tipo di informazioni, peraltro prima della conclusione del procedimento e in assenza di eventuali repliche degli interessati.

07 Maggio 2019
Relazione Annuale

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

«Una simile forma di gogna è, infatti, incompatibile con la dignità e il diritto alla riservatezza dei lavoratori».

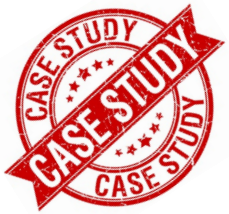
07.05.2019: Relazione Annuale 2018 – Discorso del Presidente Autorità Garante

DPIA
Videosorveglianza

La (Verifica Preliminare) DPIA nella Videosorveglianza

il Garante enuncia tutta una serie di ipotesi che vanno sottoposte a DPIA (ex verifica preliminare). Si tratta:

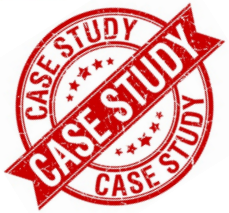
- dei **sistemi di videosorveglianza abbinati a dati biometrici**;
- degli **impianti dotati di software, che consentono il Riconoscimento delle persone**;
- dei **sistemi c.d. intelligenti**, che cioè non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli ed eventualmente registrarli;
- dei **sistemi integrati di videosorveglianza**;
- delle **casistiche di allungamento dei tempi di conservazione delle immagini** oltre il previsto termine massimo di sette giorni.



La Polizia Locale può conservare oltre i 7 giorni le immagini delle targhe dei veicoli per eventuali esigenze ?

Tempi di conservazione delle targhe dei veicoli riprese dai sistemi di Videosorveglianza della polizia municipale.

Il Corpo della polizia municipale di un Comune ha chiesto se, per corrispondere alle eventuali esigenze investigative delle Forze di polizia, era possibile prolungare fino ad un periodo di 60 giorni i tempi di conservazione delle immagini delle targhe di veicoli registrate dal sistema di videosorveglianza gestito dal Corpo medesimo.



Conservazione delle targhe dei veicoli

Tempi di conservazione delle targhe dei veicoli riprese dai sistemi di Videosorveglianza della polizia municipale.

Il **Garante** ha rilevato che il **paragrafo 3.4.** del provvedimento generale in materia di videosorveglianza, prevede che i comuni, in caso di videosorveglianza finalizzata alla tutela della sicurezza urbana, possono conservare i dati nel termine massimo di **sette** giorni successivi alla rilevazione delle immagini e che, in caso di effettive ed eccezionali esigenze di ulteriore conservazione, devono inoltrare al Garante una richiesta di verifica preliminare, adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità.

Conservazione delle targhe dei veicoli

Tempi di conservazione delle targhe dei veicoli riprese dai sistemi di Videosorveglianza della polizia municipale.

Con riferimento al caso di specie, il **provvedimento consente** quindi un prolungamento del termine di conservazione delle immagini anche in presenza di richieste della polizia giudiziaria motivate però in relazione a specifiche e puntuali attività investigative in corso, **dovendosi escludere una preventiva e generalizzata conservazione ultrasettimanale per esigenze solo eventuali. (Garante: Nota 09 dicembre 2013).**

FACE DETECTION e FACE RECOGNITION

PROVV. GARANTE 08.04.2010 § 3.2.1.

*Ad esempio, devono essere sottoposti alla verifica preliminare di questa Autorità i sistemi di videosorveglianza dotati di **software** che permetta il **riconoscimento della persona** tramite collegamento o incrocio o confronto delle immagini rilevate (es. morfologia del **volto**) con altri specifici dati personali, in particolare con dati biometrici, o sulla base del confronto della relativa immagine con una campionatura di soggetti precostituita alla rilevazione medesima.*

FACE DETECTION

Registro dei provvedimenti
n. 551 del 21 dicembre 2017

Provv. Garante

Installazione di apparati promozionali del tipo “digital signage” (definiti anche Totem) presso una stazione ferroviaria - 21 dicembre 2017 [7496252]

Totem nelle stazioni

telecamera che analizza le espressioni dei passanti

Verifica se:

nel mostrare messaggi pubblicitari, utilizzerebbero un sistema di "riconoscimento e tracciamento facciale" di coloro che si trovino davanti agli stessi.

ALGORITMI DI FACE DETECTION

La presenza di un volto verrebbe rilevata attraverso algoritmi di face detection e non di face recognition che consentirebbero quindi di rilevare (genericamente) la **presenza** di un **volto** umano **senza** però **identificarlo** attraverso caratteristiche biometriche specifiche di quel volto.

La tecnologia adottata, infatti, consentirebbe di analizzare, solamente in forma anonima e in maniera localizzata al singolo totem, **l´espressione facciale** (da felice a triste) e alcune altre caratteristiche delle persone che osservano il messaggio pubblicitario, senza conservare né trasmettere alcuna immagine o altri dati riferibili a specifici soggetti inquadrati dalla telecamera.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

ALGORITMI DI FACE DETECTION

Nonostante il sistema non consenta il riconoscimento facciale dei passanti, né il loro monitoraggio o tracciamento, e che i dati sul gradimento della pubblicità sono inviati al sistema centrale in forma totalmente anonima, **il Garante ha però accertato che l´apparecchiatura installata per effettuare l´analisi del volto di chi osserva gli annunci promozionali, anche se in locale e per un brevissimo lasso di tempo prima della immediata sovrascrittura delle immagini, effettua comunque un trattamento di dati personali funzionale all´analisi statistica dell´audience.**

Il Garante ha quindi prescritto alla società di collocare presso ogni totem installato un cartello, (anche in formato di vetrofania) che segnali la presenza della telecamera e che riporti gli elementi essenziali relativi al trattamento dei dati effettuato. Tale informativa sintetica dovrà inoltre contenere i riferimenti all´informativa completa facilmente raggiungibile – anche tramite un apposito QR Code - sul sito internet della società

FACE RECOGNITION

Videosorveglianza con funzionalità di riconoscimento facciale

Provv. 28 Luglio 2016, [doc. web. n.5386852]

TITOLARE: Ministero dell'Interno in persona del questore di Roma pro-tempore;

FUNZIONAMENTO': Il sistema è provvisto di una funzione di **riconoscimento facciale**, che fornisce le immagini degli spettatori abbinate automaticamente al nominativo della persona risultante dal sistema di controllo degli accessi ai tornelli e dal sistema di biglietteria (i dati anagrafici dell'acquirente sono richiesti al momento dell'emissione dei biglietti per assistere alle partite di calcio). Il software confronta le immagini acquisite al momento del transito nei tornelli di accesso con quelle riprese all'interno dello stadio durante gli eventi sportivi, in modo da risalire alla reale identità dell'autore di eventuali condotte delittuose

FACE RECOGNITION

Videosorveglianza con funzionalità di riconoscimento facciale

VERIFICA PRELIMINARE : La procedura di riconoscimento delle immagini tramite confronto tra quelle riprese all'interno dello stadio durante gli eventi sportivi e quelle acquisite al momento del transito nei tornelli di accesso, che fungono da campione di riferimento, configura **un trattamento di dati biometrici** che non è compreso nella casistica dei trattamenti esclusi da obbligo di **verifica preliminare** ai sensi del Provvedimento generale del Garante 12 novembre 2014 sul riconoscimento biometrico e sulla firma grafometrica (in G.U. n. 280 del 2 dicembre 2014, doc. web n. 3556992; v. anche il Provvedimento in materia di videosorveglianza 8 aprile 2010, in G.U. n. 99 del 29 aprile 2010, doc. web n. 1712680, par. 3.2.1., che individua in quali casi i trattamenti di dati personali nell'ambito di una attività di videosorveglianza devono essere sottoposti a verifica preliminare.

VIDEOSORVEGLIANZA E CONTROLLO A DISTANZA

ART. 4 STATUTO DEI LAVORATORI & ART. 114 D.lgs n.196/2003 come modificato dal D.Lgs n. 101/2018

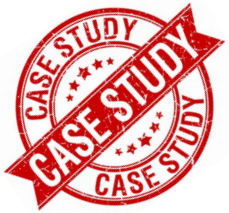
PRIMA DI INSTALLARE UN IMPIANTO DI VIDEOSORVEGLIANZA IN LUOGHI DI LAVORO CI VUOLE L'ACCORDO SINDACALE O L'AUTORIZZAZIONE DELLA D.T.L.

L'informativa ai dipendenti non esime dall'attivazione della procedura di cui all'articolo 4, dello Statuto dei Lavoratori.
Il concetto è stato ribadito recentemente in occasione di un accertamento ispettivo presso un supermercato.

LA DISCIPLINA SUL CONTROLLO A DISTANZA SI APPLICA ANCHE QUANDO LE TELECAMERE SONO INSTALLATE IN AMBIENTI DOVE IL LAVORATORE PUO'TROVARSI SALTUARIAMENTE

Cass. 6 marzo 1986, n. 1490 secondo cui il divieto di controllo a distanza dell'attività lavorativa non è escluso dal fatto che il controllo sia destinato ad essere discontinuo perché esercitato in locali dove i lavoratori possono trovarsi solo saltuariamente);

TRATTAMENTO DI DATI EFFETTUATO MEDIANTE UN SISTEMA DI VIDEOSORVEGLIANZA MOBILE
IN VIOLAZIONE DEI DIRITTI PREVISTI DALLA DISCIPLINA GIUSLAVORISTICA

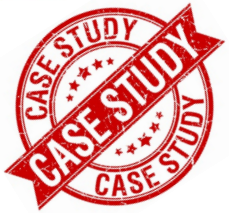


LA VIDEOSORVEGLIANZA MOBILE

SISTEMA DI VIDEOSORVEGLIANZA COSTITUITO DA TELECAMERE INSTALLATE SU AUTO DELLA POLIZIA LOCALE PER FINALITA' SIA DI SICUREZZA URBANA SIA DI SICUREZZA PUBBLICA.

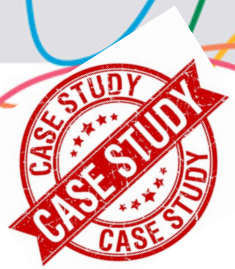
AUT. GAR. PROVV. 08.01.2015 [doc. web n. 3723437]

Registro dei provvedimenti n. 2 dell'8 gennaio 2015



AUT. GAR. PROVV. 08.01.2015 [doc. web n. 3723437]

Con segnalazione nei confronti di un Consorzio di polizia locale un Coordinamento sindacale autonomo, ha lamentato la violazione della disciplina sul controllo a distanza ex art. 4 L . N. 300/1970.



Il Sistema oggetto del Provvedimento del Garante:

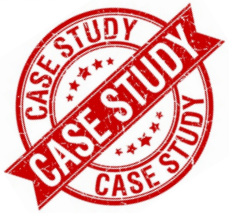
Le **telecamere**, fornite di "due obiettivi che riprendono rispettivamente in orario diurno e notturno erano posizionate sul **lato passeggero** anteriore [in modo da riprendere] la parte anteriore del veicolo [nonché] la **carreggiata** ma anche il **marciapiedi** ai lati della stessa".
La telecamera si **attiva** "in modo automatico con **l'accensione** del veicolo e resta accesa fino a **due ore dopo** lo **spegnimento.**
Il sistema è configurato in modo tale da consentire la "**trasmissione** delle **immagini** in **diretta** via internet" e, più specificamente, il comandante del corpo "poteva vedere le immagini in diretta, tanto da comunicare talvolta con gli agenti".

TITOLARE DEL TRATTAMENTO: Consorzio di Polizia Locale

FINALITA': Sicurezza Urbana e Ordine Pubblico;

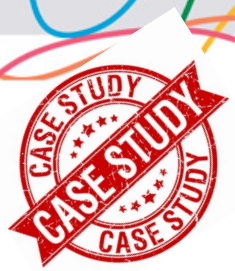
TEMPI DI CONSERVAZIONE: Le immagini registrate venivano conservate per non più di sette giorni.

ULTERIORI FUNZIONI: Il sistema non consentiva la localizzazione georeferenziata del mezzo.

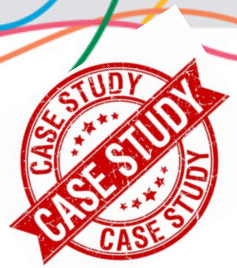


OSSERVA IL GARANTE SULLE FINALITA' PERSEGUITE DAL SISTEMA DI VIDEOSORVEGLIANZA

Con riguardo alle disposizioni del Codice applicabili, si ritiene che le **attività** che il Consorzio intende svolgere **comprendano sia** trattamenti soggetti all'ambito di applicazione dell'art. **53** del Codice, **sia** trattamenti da questo sicuramente **esclusi**. Quanto a questi ultimi si pensi, in particolare, al "monitoraggio del traffico" (punto 3.1) e alla "vigilanza sull'integrità e sulla conservazione del patrimonio pubblico e dell'ambiente" (punto 2.1, lett. a.), in relazione ai quali sono senza dubbio applicabili integralmente le disposizioni previste dal Codice.



L unicità delle **attività** di **videosorveglianza** – pur se finalizzata ad una **pluralità** di **scopi** – impone **l'integrale applicazione di tutte le norme del Codice**; conseguentemente, in assenza della informativa da rendere ai dipendenti e agli utenti, nonché della procedura di garanzia prevista dall'art. 4, comma 2, l. n. 300/1970, si ritiene che **il trattamento effettuato mediante il sistema di videosorveglianza . . . . sia avvenuto in violazione degli artt. 13 e 11, comma 1, lett. a) in relazione all'art. 114 del Codice** e che debba, pertanto, essere dichiarato illecito nella parte in cui risulti finalizzato a scopi non ricompresi nell'art. 53 del Codice.



COSA FARE PER ADOTTARE QUESTO SISTEMA

qualora la pubblica amministrazione intenda in futuro riprendere il suddetto trattamento, quest'ultimo potrà dunque svolgersi:

a. previa idonea **informativa** da rendere ai **dipendenti** ai sensi dell'art. 13 del Codice;

b. osservando, ai sensi dell'art. 13 del Codice, l'obbligo di **informare** gli **interessati** che stanno per accedere in una zona videosorvegliata (se del caso anche apponendo adeguata cartellonistica all'inizio dei comuni interessati o comunque utilizzando altri strumenti appropriati, ad esempio fornendo utili elementi informativi all'interno dei siti istituzionali dei Comuni interessati e del Consorzio stesso);

c. previa effettuazione delle procedure di garanzia previste **dall'art. 4**, comma 2, l. **300/1970** (accordo con le rappresentanze sindacali aziendali oppure, in difetto di accordo, autorizzazione rilasciata dalla competente Direzione Territoriale del Lavoro; cfr. provv. 9.2.2012, n. 56, doc. web n. 1886999).

INL
CIRCOLARE N. 5 DEL 19 FEBBRAIO 2018

Oggetto: indicazioni operative sull'installazione e utilizzazione di impianti audiovisivi e di altri strumenti di controllo ai sensi dell'art. 4 della legge n. 300/1970.

INL: CIRCOLARE N. 5 DEL 19 FEBBRAIO 2018

Si deve allegare la planimetria con l'esatto numero delle telecamere da installare ?

NO →

«non appare fondamentale specificare il posizionamento predeterminato e l'esatto numero delle telecamere da installare fermo restando, comunque, che le riprese effettuate devono necessariamente essere **coerenti e strettamente connesse con le ragioni legittimanti il controllo** e dichiarate nell'istanza, ragioni la cui effettiva sussistenza va sempre verificata in sede di eventuale accertamento ispettivo»

perché ? →

in quanto lo stato dei luoghi e il posizionamento delle merci o degli impianti produttivi è spesso oggetto di continue modificazioni nel corso del tempo (si pensi ad esempio alla rotazione delle merci nelle strutture della grande distribuzione) e **pertanto rendono scarsamente utile una analitica istruttoria basata su planimetrie che nel corso del breve periodo non sono assolutamente rappresentative del contesto lavorativo**.

INL: CIRCOLARE N. 5 DEL 19 FEBBRAIO 2018

Con quale misura di sicurezza deve avvenire l'accesso alle immagini?

L'accesso alle immagini registrate, sia da remoto che "in loco", deve essere necessariamente tracciato anche tramite apposite funzionalità che consentano la conservazione dei "log di accesso"per un congruo periodo, non inferiore a sei mesi

Ci vuole sempre la doppia chiave fisica o logica ?

NO

«Non va più posta come condizione, nell'ambito del provvedimento autorizzativo, l'utilizzo del sistema della "doppia chiave fisica o logica"»

REGOLE:

SI CONTRO ATTI VANDALICI

RIPRESE CIRCOSCRITTE ALLE SOLE AREE INTERESSATE

IMPIANTI ATTIVI IN ORARI DI CHIUSURA DEGLI ISTITUTI

L'eventuale installazione di sistemi di videosorveglianza presso istituti scolastici deve garantire "il diritto dello studente alla riservatezza" (art. 2, comma 2, d.P.R. n. 249/1998), prevedendo opportune cautele al fine di assicurare l'armonico sviluppo delle personalità dei minori in relazione alla loro vita, al loro processo di maturazione ed al loro diritto all'educazione (§ 4.3. Provv. 08.04.2010)

In tale quadro, può risultare ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate ed attivando gli impianti negli orari di chiusura degli istituti; è vietato, altresì, attivare le telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche che si svolgono all'interno della scuola (§ 4.3.1. Provv. 08.04.2010)

videosorveglianza negli asili e nelle strutture per anziani e disabili.

Il **disegno di legge** approvato dalla Camera (ora passa all'esame del Senato) prevede e regola, all'art. 4, la videosorveglianza negli asili e nelle strutture per anziani e disabili.
Il Ddl prevede che le **immagini siano criptate**, per proteggerle dalla visualizzazione da parte di terzi
L'accesso alle registrazioni sarà consentito solo al pubblico ministero e, su sua delega, alla **polizia giudiziaria**, per lo svolgimento di indagini su reati in danno dei minori o delle persone ospitate nelle strutture. Nei casi di urgenza la polizia giudiziaria potrà accedere alle registrazioni dandone immediata comunicazione al pubblico ministero.
Fuori dalle predette ipotesi (notizia di reato e visione delle registrazioni da parte dell'autorità giudiziaria), le immagini filmate non potranno essere viste da nessun altro, neppure dal personale della scuola.
Per l'installazione del sistema di videosorveglianza sarà necessario l'assenso dei sindacati e la presenza dei sistemi di videosorveglianza dovrà essere segnalata con dei cartelli a tutti quelli che accedono negli edifici monitorati.
Il provvedimento non si occupa solo di videosorveglianza ma anche di formazione e delega il governo ad "adottare un decreto legislativo in materia di valutazione attitudinale nell'accesso alla professioni educative e di cura" ovvero test psico-attitudinali da fare al momento dell'assunzione e poi periodicamente, "nonché di formazione iniziale e permanente del personale delle strutture" (art. 2).

COSA SI RISCHIA SE NON RISPETTO LA NORMATIVA ?

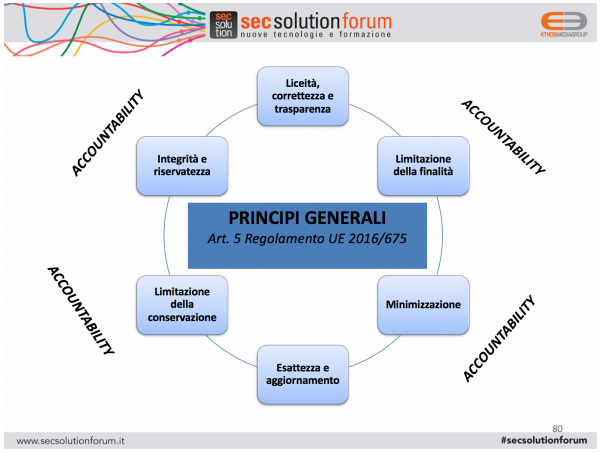
ART. 83, Paragrafo 4 GDPR

Sono soggette a sanzioni amministrative **fino a 10 milioni di euro**, o in caso di un'impresa, fino **al 2% del fatturato totale annuo mondiale** dell'esercizio precedente, le violazioni delle disposizioni relative agli obblighi del Titolare o del Responsabile di cui agli articoli:

- 7 (consenso dei minori),
- 11 (trattamenti che non richiedono l'identificazione degli interessati),
- 25 (privacy by design e privacy by default),
- 26 (cotitolarità del trattamento),
- 27 (nomina rappresentante del Titolare non stabilito nell'Unione Europea),
- 28 (Responsabili del trattamento),
- 29 (istruzioni e autorità del Titolare),
- 30 (documentazione relativa a ciascun trattamento di dati personali),
- 31 (cooperazione con l'autorità di vigilanza),
- 32 (sicurezza del trattamento),
- 33 (notificazione dei data breach all'autorità),
- 34 (comunicazione dei data breach agli interessati),
- 35 (DPIA – Data Protection Impact Assessment),
- 36 (consultazione preventiva dell'autorità di vigilanza),
- 37,38 e 39 (designazione, posizione e compiti del DPO – Data Protection Officer),
- 40- 43 (processi di certificazione).

ART. 83, Paragrafo 5 GDPR

Sanzioni amministrative fino a 20 milioni di euro, o in caso di un'impresa, fino al 4% del fatturato totale annuo mondiale dell'esercizio precedente, sono invece previste per le violazioni in materia di **principi base del trattamento**, condizioni per il consenso, diritti degli interessati, trasferimento di dati personali all'estero, mancata ottemperanza a un ordine o a una limitazione temporanea o definitiva del trattamento disposti dall'autorità di vigilanza.



Il Titolare del trattamento, allorquando svolge una valutazione d'impatto privacy si consulta con il Data Protection Officer (Art. 35, § 2 GDPR)

COMPITI - Art. 39

- ✓ Coinvolto in questioni riguardanti la protezione dei dati (art. 38^{1});
- ✓ Informa e fornisce consulenza al Titolare, ai responsabili del trattamento nonché ai dipendenti (art. 39^{1a}).

- ✓ Sorveglia l'osservanza della normativa in tema di protezione dei dati personali (art. 39^{1b});
- ✓ Vigila l'osservanza dei processi interni (art. 39^{1b})

- ✓ Cooperare con l'Autorità Garante (art. 39^{1d});
- ✓ Fungere da punto di contatto con l'Autorità Garante (art. $39^{1^{\circ}}$)

Deve essere consultato dal Titolare nei casi di Valutazione di impatto privacy e rendere un parere (art. 35^{2} e 39^{1c})

Grazie
per l'attenzione!

Continua a seguirci su
www.secsolutionforum.it